COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

PATRICK W. FINNERTY
DIRECTOR

SUITE 1300
600 EAST BROAD STREET
RICHMOND, VA 23219
804/786-7933
800/343-0634 (TDD)
www dmas virginia gov

TO: Patrick W. Finnerty
Director, DMAS

FROM: Security Advisory Committee (SAC)

DATE: May 21, 2007

RE: Information Security and HIPAA Security Policies, 2007

The SAC has reviewed, approved and recommends that you authorize issuance of the Information Security and HIPAA Security Policies (attached):

APPROVED Barbara C Newlin DATE 5-21-07
Barbara Newlin, Human Resources Director

APPROVED Sylvia Hart DATE 5/18/07
Sylvia Hart, Information Management Director

APPROVED Scott Crawford DATE 5/18/07
Scott Crawford, Deputy Director for Finance and Administration

APPROVED John M. Karabaic DATE 5/18/07
John Karabaic, Compliance, and Security Officer

****

Authorized P W Finnerty DATE 5/21/07
Patrick W. Finnerty, Director, DMAS

COMMONWEALTH OF VIRGINIA

Department of Medical Assistance Services (DMAS) Information Technology Security Policy

ITRM PUBLICATION VERSION CONTROL

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to DMAS' Compliance and Security Office (OCS) or Information Management (IM) Division. DMAS will issue an update as appropriate.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	May 21, 2007	Base Document

PREFACE

Publication Designation
DMAS IT Security Policy SEC2007-01

Subject
Information Technology Security Policy

Effective Date
May 21, 2007

Compliance Date
Immediate

Supersedes where applicable:*
DMAS ITRM # 93-1 Information Security Plan
DMAS ITRM #93-1 Risk Assessment
DMAS ITRM #93-2 Computer Security
DMAS ITRM #93-2 Information Security Officer
DMAS ITRM #93-3 Information Systems Management Access
DMAS ITRM #93-4 Incident Monitoring
DMAS ITRM #93-5 Information Systems Security Access
DMAS ITRM #93-5 Computer (Micro) Backup and Security
DMAS ITRM #93-6 Security Awareness Training
DMAS ITRM #93-7 Physical Security Access Controls
DMAS ITRM #93-8 Environmental Protection Controls
DMAS ITRM #93-9 System Development Manual
DMAS ITRM #93-10 Local Area Network Controls
DMAS ITRM #93-12 Fiscal Agent Controls
DMAS ITRM #93-13 Operational Controls
DMAS ITRM #93-14 Contingency Management Plan
DMAS ITRM #93-15 Disaster Recovery Plan

*Some components of the above may still be in place until demoted to procedure levels

Scheduled Review
DMAS Security Advisory Council
One (1) year from effective date

Authority
Code of Virginia, § 2.2-603(F)
(Authority of Agency Directors)

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA"; Appointment of Chief Information Officer [CIO])

Code of Virginia, §2.2-2827
(Restrictions on state employee access to information infrastructure)

Code of Virginia, §2.2-3800
(Government Data Collection and Dissemination Practices Act)

Scope
This policy is applicable to Department of Medical Assistance Services (DMAS) (also known as Agency) that manages, develops, purchases, and uses information technology resources at DMAS.

Purpose
To protect the Commonwealth information technology assets and the information processed by defining the minimum information technology security program for DMAS.

Precedence
Precedence of Information Security Policies vs. HIPAA: DMAS must comply with both the Federal HIPAA Security Rule and the Commonwealth of Virginia Information Technologies (VITA) Policies and Standards. In the event of a conflict between DMAS HIPAA Security Policies, developed to comply with the HIPAA Security Rule, and DMAS Information Security Policies, developed to comply with VITA requirements, the more stringent policy will apply.

General Responsibilities
(Italics indicate quote from the Code of Virginia requirements)

Chief Information Officer of the Commonwealth
In accordance with *Code of Virginia*, § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits."*

Chief Information Security Officer
The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures and standards to protect the confidentiality, integrity, and availability of the Commonwealth's information assets

Council on Technology Services
In accordance with the *Code of Virginia* § 2.2-2009, the Council on Technology Services is assigned the following duties: *"In developing and updating such policies, procedures and standards, the CIO shall consider, at a minimum, the advice and recommendations of the Council on Technology Services."*

Technology Strategies and Solutions Directorate
In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the Technology Strategies and

Solutions Directorate the following duties: *Develop and adopt policies, standards and guidelines for managing information technology by state agencies and institutions.*"

All State Agencies

In accordance with the *Code of Virginia* § 2.2-603, § 2.2-2009, and § 2.2-2010 all State Agencies are responsible for complying with Commonwealth ITRM policies and standards and considering Commonwealth ITRM guidelines issued by the CIO. In addition: "*The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence.*"

Regulatory References

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA).
2. Privacy Act of 1974.
3. Children's Online Privacy Protection Act
4. Family Educational Rights and Privacy Act
5. Executive Order of Critical Infrastructure Protection.
6. Federal Child Pornography Statute: 18 U.S.C. & 2252
7. Bank Secrecy Act.
8. Virginia Computer Crime Act, *Code of Virginia*, §18.2-152.3, .4, 5, and 6
9. Library of Virginia Records Management Program, *Code of Virginia*, Title 42.1, Chapter 7, sec 42.1-85.
10. Federal Information Security Management Act (FISMA).
11. Office of Management and Budget (OMB) Circular A-130.

International Standards

1. International Standard, Information Technology – code of practice for information security management, BS ISO/IEC 17799:2005
2. **Orange Book**

Definitions

See Glossary

Related ITRM Standard

ITRM Standard SEC501-01: Information Technology Security Standard (Revised July 1, 2006)
DMAS IT Security Standard xxxx-xx (in draft)

TABLE OF CONTENTS

1. INFORMATION TECHNOLOGY (IT) SECURITY POLICY STATEMENT

1.1 Background

The Commonwealth of Virginia (COV) along with the Department of Medical Assistance Services (DMAS) relies heavily on the application of information technology (IT) for the effective delivery of government services. Rapid and continuing technical advances have increased the dependence of DMAS on IT DMAS data, software, hardware, and telecommunications are recognized as important resources and must be protected through Agency IT security programs.

DMAS' IT security programs shall be built on the concept of public trust. DMAS' IT security program provides sustainability — a consistent approach to IT security that can be replicated across networks, applications, and transactions. The DMAS IT Security Program provides the generally acceptable principles and practices for DMAS to use in securing its IT systems and data.

1.2 Guiding Principles

The following principles guide the development and implementation of the DMAS IT Security Program.

a. DMAS Data is:

   1. A critical asset that shall be protected;

   2. Restricted to authorized personnel for official use.

b. IT security must be:

   1. A cornerstone of maintaining public trust;

   2. Managed to address both business and technology requirements;

   3. Risk-based and cost-effective;

   4. Aligned with COV and DMAS priorities, industry-prudent practices, and government requirements;

   5. Directed by policy but implemented by business owners;

   6. The responsibility of all users of DMAS' IT systems and data.

1.3 Statement of Policy

It remains the policy of the COV that the Agency Head is responsible for the security of the Agency's data and for taking appropriate steps to secure Agency IT systems and data through the development of an Agency IT security program as stated both in this policy and the [VITA] *Information Technology Security Policy* (COV ITRM Policy SEC500-02).

This policy and related standards provide the minimum requirements for DMAS' IT security program to be implemented in a framework relative to information risk. The Agency Head may establish additional, more restrictive IT security programs and related policies but must, at a minimum, meet the requirements of this policy and the related standards. If, in the sole judgment of a Division Director, the Agency cannot meet one or more of the minimum requirements, a request for an exception shall be made in writing to the Security Advisory Committee via the exception process for consideration. This process is described in more detail in Section 7 of this document, as well as in Section 1.5 of the [VITA] *Information Technology Security Standard* (COV ITRM Standard 501-01). The form that an Agency must submit to request an exception to any requirement of this policy or the related Standards is attached as an Appendix to this document.

Precedence of Information Security Policies vs. HIPAA: DMAS must comply with both the Federal HIPAA Security Rule and the Commonwealth of Virginia Information Technologies (VITA) Policies and Standards. In the event of a conflict between DMAS HIPAA Security Policies, developed to comply with the HIPAA Security Rule, and DMAS Information Security Policies, developed to comply with VITA requirements, the more stringent policy will apply.

The function of this policy is to protect DMAS IT systems and data from credible threats, whether internal or external, deliberate or accidental. It is the policy of DMAS to use all reasonable IT security control measures to:

a. Protect DMAS data against unauthorized access and use;

b. Maintain integrity of DMAS data;

c. Meet requirements for availability of data residing on IT systems;

d. Meet federal (including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules), state and other regulatory and legislative requirements.

The remainder of this policy is divided into seven sections that define the requirements for the DMAS' IT security program.

a. Section 2 addresses key roles and responsibilities of managers to provide IT security measures and controls to protect the DMAS IT systems and data.

b. Section 3 addresses the DMAS IT Security Program and outlines the IT security subprograms.

c. Section 4 addresses IT security compliance and proper administration of DMAS' IT Security Program with program management oversight.

d. Section 5 addresses IT security audits to test for adequacy of controls and assess the level of compliance with established policies, standards, or procedures. Section 5 also summarizes the [VITA] *IT Security Audit Standard* (COV ITRM Standard SEC502-00) which provides specific IT security audit requirements for Agencies, which are summarized in this section.

e. Section 6 defines 'DMAS' policy for the confiscation and removal of IT resources.

f. Section 7 describes the process for requesting an exception to the requirements of this policy and the related standards.

g. Section 8 contains a glossary of IT security definitions.

h. Section 9 contains a list and description of IT security acronyms and the terms to which they refer.

2. KEY IT SECURITY ROLES AND RESPONSIBILITIES

IT security roles and responsibilities are assigned to individuals, and may differ from the COV role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. Additional information concerning the assignment of multiple IT security roles is contained in section 2.2 of the [VITA] *IT Security Standard* (COV ITRM Standard SEC501-01).

2.1 Chief Information Officer of the Commonwealth (CIO)[at VITA]

The *Code of Virginia* §2-2.2009 states that *"the CIO* [at VITA] *shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications."*

2.2 Chief Information Security Officer (CISO) [at VITA]

The CISO [at VITA] is responsible for development and coordination of the COV IT Security Program and, as such, performs the following duties:

a. Administers the COV IT Security Program and periodically assesses whether the program is implemented in accordance with COV IT Security Policies and Standards.

b Reviews requested exceptions to COV IT Security Policies, Standards and Procedures.

c. Provides solutions, guidance, and expertise in IT security.

d. Maintains awareness of the security status of sensitive IT systems.

e. Facilitates effective implementation of COV IT Security Program, by:

   i. Preparing, disseminating, and maintaining IT security, policies, standards, guidelines and procedures as appropriate;
   ii. Collecting data relative to the state of IT security in the COV and communicating as needed;
   iii. Providing consultation on balancing an effective IT security program with business needs.

f. Provides networking and liaison opportunities to Information Security Officers (ISOs).

2.3 Agency Head

DMAS' Agency Head is responsible for the security of DMAS' IT systems and data. The Agency Head's IT security responsibilities include the following:

a. Comply with VITA policies, standards and the HIPAA Privacy and Security Rules.

b. Designate via e-mail to VITASecurityServices@vita.virginia.gov an ISO for the Agency and providing the person's name, title and contact information to VITA no less than biennially. DMAS will designate at least one backup for the ISO, as well.

c. Determine the optimal place of the IT security function within the Agency hierarchy with the shortest practicable reporting line to the Agency Head.

d. Maintain an Agency IT security program that is sufficient to protect the Agency's IT systems, and that is documented and effectively communicated.

e. Review and approve the Agency's Business Impact Analyses (BIAs), a Risk Assessment (RA), and a Continuity of Operations (COOP) Plan, to include an IT Disaster Recovery Plan, if applicable.

f. Accept residual risk as described in section 2.5 of the [VITA] *IT Security Audit Standard* (COV ITRM Standard SEC502-00).

g. Maintain compliance with [VITA] *IT Security Audit Standard* (COV ITRM Standard SEC502-00). This compliance must include, but is not limited to:

- Requiring development and implementation of an Agency plan for IT security audits, and submitting this plan to the CISO;
- Requiring that the planned IT security audits are conducted;
- Receiving reports of the results of IT security audits;
- Requiring development of Corrective Action Plans to address findings of IT security audits; and
- Reporting to the CISO all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings.

h. Facilitate the communication process between data processing staff and those in other areas of the Agency.

i. Establish a program of IT security safeguards.

j. Establish an IT security awareness and training program.

k. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.

DMAS Division Directors and Managers at all levels shall provide for the IT security needs under their jurisdiction. They shall take all reasonable actions to provide adequate IT security and to escalate problems, requirements, and matters related to IT security to the highest level necessary for resolution.

2.4 Information Security Officer (ISO) and Backup Information Security Officer (backup ISO) (IM Security Engineer)

The ISO and backup ISO (IM Security Engineer) are responsible for developing and managing DMAS' IT security program. Both are known as the "ISO". The ISO's duties are as follows:

a. Comply with VITA policies, standards and the HIPAA Privacy and Security Rules.

b. Develop and manage the IT security program at DMAS that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk.

c. Develop and maintain an IT security awareness and training program for DMAS staff, including contractors and IT service providers.

d. Coordinate and provide IT security information to the [VITA] CISO as required.

e. Implement and maintain the appropriate balance of protective, detective and corrective controls for DMAS' IT systems commensurate with data sensitivity, risk and systems criticality.

f. Mitigate and report all IT security incidents in accordance with §2.2-603 of the *Code of Virginia* and VITA requirements and take appropriate actions to prevent recurrence.

g. Maintain liaison with the [VITA] CISO.

2.5 Privacy Officer

DMAS must have a Privacy Officer as required by law or regulation. The Privacy Officer provides guidance on and:

a. Ensures the ongoing identification of compliance risks, and remediation of same to remain in compliance with federal HIPAA regulations and state laws.

b. The continued process of identification of the facility's physical safeguards, and computer system network components required to ensure the protection, privacy and security of health information.

c. Security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

d. The continuous review and update of DMAS divisional, HIPAA specific, policies and processes and procedures relative to the care, custody, privacy, security and protection of health information.

e. The identification and implementation of a continuous HIPAA Privacy education process for DMAS' workforce, and an awareness program for DMAS Business Associates and notification to Providers.

f. The review and continuous monitoring of all Business Associate agreements (BAA) that involve the management of protected health information for DMAS. These agreements

require specific amendments, or attachments be in place that specify the protocols necessary to the continued protection, and minimal necessary use of protected health information to conduct business on behalf of DMAS, and to transmit protected health information in an electronic format and means.

2.6 System Owner

The System Owner is the DMAS Division Director, manager or designee responsible for operation and maintenance of a DMAS IT system. With respect to IT security, the System Owner's responsibilities include the following:

a. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.

b. Identify system risk and develop any additional IT security procedures required to protect the system in a manner commensurate with risk.

c. Maintain compliance with DMAS IT security policies, standards and procedures in all IT system activities.

d. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.

e. Designate a System Administrator for the system.

2.7 Data Owner

The Data Owner is the DMAS Division Director, manager, or designee responsible for the operational decisions regarding data, and is responsible for the following:

a. Evaluate and classify sensitivity of the data.

b. Identify protection needs of the data based on the sensitivity classification of the data, any legal or regulatory requirements, and business needs.

c. Communicate data protection requirements to the System Owner.

d. Define requirements for access to the data subject to approval by the System Owner.

2.8 Data Custodian

Data Custodians are individuals in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

a. Protect the data in their possession from unauthorized access, alteration, destruction, or usage.

b. Operate and monitor IT systems in a manner consistent with DMAS' IT security policies and standards.

c. Provide data owners with reports, when necessary and applicable.

2.9 IM Security Engineer

The IM Security Engineer (backup ISO) performs the following:

a. Provides logical access control in accordance with policies in place and system owner/data owner direction.

b Documents processed access requests along with reviews for exceptional access requests with the system owner or data owner for approval or denial along with documenting the results.

c. Ensures access is granted in accordance with system owner's or data owner's intentions, DMAS policies or other policies DMAS must comply with.

2.10 System Administrator

System Administrators may be a designated analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the IM Security Engineer in support of the System Owner, Data Owner, and/or Data Custodian. System Administrators assist DMAS management in the day-to-day administration of DMAS IT systems and perform the following:

a. Implements security controls and other requirements of the DMAS IT security program on IT systems for which the System Administrator have been assigned responsibility.

2.11 IT System Users

All users of DMAS IT systems including employees and contractors are responsible for the following:

a. Read and comply with DMAS IT security program requirements.

b. Report breaches of IT security, actual or suspected, to DMAS management and/or the ISO.

c. Take reasonable and prudent steps to protect the security of DMAS IT systems and data to which they have access.

3. IT SECURITY PROGRAM

The ISO and backup ISO is charged with developing and administering DMAS' IT Security Program in accordance with the policies reviewed and approved by the Security Advisory Committee and authorized by the Director of DMAS (Agency Head). DMAS' ISO is charged with developing and administering the IT security program at DMAS in a manner that meets DMAS' business needs, protects IT systems and data in a manner commensurate with data sensitivity and risk, and, at a minimum, meets the requirements of COV and HIPAA policies and standards (see Appendix 2).

3.1 IT Security Program Components

The policy of DMAS is to secure its IT systems using methods based on the sensitivity of the data processed and the risks to which the systems and data are subject, including the dependence of critical Agency business processes on the data and systems.

The components described below provide the basis for designing DMAS' IT security program and safeguards. They do not represent organizational functions within the IT security program, but rather the functional components of the IT security program (see Appendix 1).

3.1.1 Risk Assessment (RA) and Management

As previously stated, this policy and related standards are based on protecting DMAS IT systems and data based on sensitivity and risk, including system availability needs. Accordingly, Risk Assessment (RA) and Management is a central component of an Agency IT security program and allows DMAS to determine how these factors apply to its IT systems

The first step in Risk Management is a Business Impact Analysis (BIA). BIA is a process of analyzing Agency business functions, to identify those that are essential or those that contain sensitive data, and assessing the resources that support them. For the purposes of IT security, the BIA identifies those business functions that are essential or involve sensitive data and that are dependent on IT. This analysis is necessary in order to determine the appropriate level of protection for IT systems and the data they process.

After completing the BIA, DMAS documents and characterizes the types of data it handles, and classifies the sensitivity of its IT systems and data for use in the RA process. Sensitivity must consider the elements of availability, confidentiality and integrity.

DMAS then defines, inventories, and determines ownership all of its IT systems classified as sensitive so that IT security roles can be appropriately assigned

A periodic RA is required for all DMAS IT systems. The RA process assesses the threats to DMAS IT systems and data, probabilities of occurrence and the appropriate IT security controls necessary to reduce these risks to an acceptable level.

After appropriate mitigating IT security controls have been applied relative to sensitivity and risk, based on RA results, DMAS IT systems require periodic, independent IT Security Audits. These audits are necessary to determine whether the overall protection of DMAS IT systems and the data it handles is adequate and effective. The requirements for IT Security Audits are discussed in more detail in Section 5 of this document, and in the [VITA] *IT Security Audit Standard* (COV ITRM Standard SEC502-00).

IT Security Audits may identify additional required mitigating controls for sensitive DMAS IT systems in order to provide adequate and effective protection of the systems and the data it handles. After applying these controls, the final step in the RA process is formal acceptance by the Agency Head or designee of any residual risk to DMAS operations from DMAS IT systems.

3.1.2 IT Contingency Planning

IT Contingency Planning defines processes and procedures that plan for and execute recovery and restoration of IT systems and data that support essential business functions if an event occurs that renders the IT systems and data unavailable. IT Contingency Planning includes IT Disaster Recovery Planning, and IT System Backup and Restoration to normal operations.

IT Disaster Recovery (DR) Planning supports Continuity of Operations (COOP) Planning by defining specific procedures and processes for restoring IT systems and data that support essential business functions, on a schedule that supports DMAS mission requirements.

Based on related elements in the IT contingency planning process, IT System Backup and Restoration includes plans and restoration schedules that meet DMAS mission requirements for the backup and restoration of data

3.1.3 IT Systems Security

The purpose of IT systems security is to provide adequate and effective protection for DMAS IT systems in the areas of IT System Hardening, IT Systems Interoperability Security, Malicious Code Protection, and IT Systems Development Life Cycle Security. DMAS IT systems may require further security controls for adequate protection based on the identification of sensitivity and risk to these systems, including system availability needs, identified through RA procedures and processes. In addition, some security controls are necessary, independent of sensitivity and risk.

3.1.4 Logical Access Control

Logical Access Control protects the confidentiality, integrity, and availability of DMAS IT systems and data against compromise. Logical Access Control requirements identify the measures needed to verify that all IT system users are who they say they are and that they are permitted to use the systems and data they are attempting to access. Logical Access Control includes Account Management, Password Management, and Remote Access.

3.1.5 Data Protection

Data Protection provides security safeguards for the processing and storing of data. This component of the DMAS IT Security Program outlines the methods that DMAS uses to safeguard data in a manner commensurate with the sensitivity and risk of the data stored. Data Protection includes Media Protection and Encryption.

3.1.6 Facilities Security

Facilities Security safeguards for the space leased by DMAS at its primary location at the 600 East Broad Street facility require planning and application of facilities security practices. Safeguards include (but are not limited to) a first line of defense for IT systems against damage, theft, unauthorized disclosure of data, loss of control over system integrity, and interruption to computer services.

3.1.7 Personnel Security

Personnel Security controls reduce risk to DMAS IT systems and data by applying Access Determination and Control to restrict access to these systems and data to those individuals who require such access as part of their job duties (see 3.1.4 Logical Access Control). Personnel Security also includes Security Awareness and Training requirements to provide all IT system users with appropriate understanding regarding DMAS IT security policies and Acceptable Use requirements for DMAS IT systems and data.

3.1.8 Threat Management

Threat Management addresses protection of DMAS IT systems and data by preparing for and responding to IT security incidents. This component of the DMAS IT Security Program includes Threat Detection, Incident Handling, and IT Security Monitoring and Logging.

3.1.9 IT Asset Management

DMAS IT Asset Management includes protection of the components that comprise DMAS IT systems by managing them in a planned, organized, and secure fashion. Asset Management also includes IT Asset Control, Software License Management, Configuration Management and Change Control as defined and administered by the VITA-Northrup-Grumman Partnership.

4. COMPLIANCE

DMAS measures compliance through processes that include, but are not limited to:

- inspections, reviews, and evaluations;
- monitoring;
- audits; and
- confiscation and removal of IT systems and data.

4.1 Monitoring

4.1.1 General Monitoring Activities

Monitoring is used to improve IT security, to assess appropriate use of DMAS IT resources, and to protect those resources from attack. Use of DMAS IT resources constitutes permission to monitor that use. There is no expectation of privacy when utilizing DMAS IT resources. DMAS reserves the right to:

a. Review the data contained in or traversing COV IT resources.

b. Review the activities on COV IT resources.

c. Act on information discovered as a result of monitoring and disclose such information to law enforcement and other organizations as deemed appropriate by the Agency Head, ISO, or other DMAS management as needed.

4.1.2 User Agreement to Monitoring

Any use of DMAS IT resources constitutes consent to monitoring activities that may be conducted whether or not a warning banner is displayed. Users of DMAS IT resources:

a. Agree to comply with DMAS policy concerning the use of IT resources;

b. Acknowledge that their activities may be subject to monitoring;

c. Acknowledge that any detected misuse of DMAS IT resources may be subject to disciplinary action and legal prosecution.

4.1.3 Internet Privacy

DMAS complies with the *Code of Virginia* § 2.2-3803 (B) requiring every public body in the COV that has an Internet website to develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public and is consistent with the requirements of the *Code*.

4.1.4 User Monitoring Notification

Where possible, all IT system users will be notified by the display of an authorized DMAS warning banner that DMAS IT systems may be monitored and viewed by authorized personnel, regardless of privacy concerns. This notice shall, at a minimum, appear whenever the IT system user first logs on to the IT system and shall be included in IT security awareness training.

4.1.5 What is Monitored?

Monitoring of DMAS IT systems and data may include, but is not limited to, network traffic; application and data access; user commands; email and Internet usage; and message and data content.

4.1.6 Requesting and Authorizing Monitoring

The Agency Head, ISO (or other DMAS designee) when appropriate has the responsibility to authorize monitoring or scanning activities for network traffic, application and data access, keystrokes, user commands, and email and Internet usage for COV and DMAS IT systems and data. The ISO shall notify the [VITA] CISO when appropriate.

4.1.7 Infrastructure Monitoring

DMAS IT personnel are responsible for maintaining security in their environment through the following processes:

a. Monitoring all systems for security baselines and policy compliance.

b. Notifying DMAS ISO of any detected or suspected incidents.

c. Monitoring their environment infrastructure.

Note that installation or usage of unauthorized monitoring devices is strictly prohibited.

5. IT SECURITY AUDITS

5.1 Description

DMAS complies with *the Code of Virginia* § 2.2-2009 giving the [VITA] CIO the responsibility to *"direct the development of policies, procedures and standards for . . . performing security audits of government databases and data communications."* These policies are outlined in this section; specific requirements are detailed in the [VITA] *IT Security Audit Standard* (COV ITRM Standard SEC502-00).

5.2 Performance of IT Security Audits

As required by the [VITA] *IT Security Audit Standard* (COV ITRM Standard SEC502-00), IT Security Audits (audits) may be conducted by CISO personnel, DMAS Internal Auditors, the Auditor of Public Accounts, or staff of a private firm that, in the judgment of DMAS, has the experience and expertise required to perform IT security audits.

Annually, DMAS will develop and submit to the [VITA] CISO an audit plan for Agency government databases and data communications. Strictly speaking, a government database is a collection of DMAS data organized into interrelated tables and specifications of data objects.

Audits conducted under the annual DMAS Audit Plan must measure compliance with the [VITA] *Information Technology Security Policy* (COV ITRM Policy SEC500-02) and the [VITA] *Information Technology Security Standard* (COV ITRM Standard SEC501-01) IT Security Auditors should also use standards that measure compliance with any other applicable federal (HIPAA) and state regulations.

5.3 Documentation and Reporting of IT Security Audits

After conducting the audit, the auditor shall report the audit results to the DMAS' Internal Audit Division. Internal Audit shall then require the development of a Corrective Action Plan (CAP) that includes concurrence or non-concurrence with each finding in the audit report as well as the mitigation strategies. The CAP will then be presented to the Agency Head in accordance with the [VITA] *IT Security Audit Standard* (COV ITRM Standard SEC502-00). The Agency Head or designee shall submit to the [VITA] CISO a report containing a record of all IT Security Audits conducted by or on behalf of DMAS. The report must include all findings and specify whether DMAS concurs or does not concur with each The report must also include the status of outstanding corrective actions for all IT Security Audits previously conducted by or on behalf of DMAS.

6. PROTECTION OF IT RESOURCES

6.1 Confiscation and Removal of IT Resources

The Agency Head in compliance with the [VITA] CISO through DMAS' ISO (or designee) or other Administration (or designee) authorities as necessitated by circumstances, may authorize the

confiscation and removal of any IT resource suspected to be the object of inappropriate use or violation of COV IT security laws or policies to preserve evidence that might be utilized in forensic analysis of a security incident.

7. PROCESS FOR REQUESTING EXCEPTION TO IT SECURITY POLICY

If a Division Director determines that compliance with this policy or related standards would result in a significant adverse impact to the Agency, the Division Director may request approval from the DMAS Security Advisory Committee (SAC) to deviate from the specific security requirement by submitting an exception request to the SAC (see the form attached as Appendix 3 to this document).

Each request shall be in writing to the SAC. Included in each request shall be a statement (and attachments as needed) detailing the reasons for the exception and compensating controls.

8. GLOSSARY OF IT SECURITY DEFINITIONS

Access: The ability or permission to enter or pass through an area or to view, change, or communicate with an IT system.

Access Controls: A set of procedures performed by hardware, software, and administrators to monitor access, identify all IT system users requesting access, record access attempts, and prevent unauthorized access to IT systems and data. Account an established relationship between a user and an IT system.

Accountability: The association of each logon ID with one and only one user within each IT system, so that the user can always be tracked while using an IT system, providing the ability to know which user performed what system activities.

Agency Head: The chief executive officer of a department established in the executive branch of the Commonwealth of Virginia

Alert: Advance notification that an emergency or disaster situation may occur

Application: A computer program or set of programs that meet a defined set of business needs. See also *Application System*

Application System: An interconnected set of IT resources under the same direct management control that meets a defined set of business needs. See also *Application, Support System*, and *Information Technology (IT) System*

Asset: Any software, data, hardware, administrative, physical, communications, or personnel resource.

Attack: An attempt to bypass security controls on an IT system. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT system and the effectiveness of existing countermeasures

Audit: An independent review and examination of records and activities to test for adequacy of controls, measure compliance with established policies and operational procedures, and recommend changes to controls, policies, or procedures.

Authenticate: To determine that something is genuine. To reliably determine the identity of a communicating party or device.

Authentication: The process of verifying the identity of a station, originator, or individual to determine the right to access specific types of data. In addition, a measure designed to protect against fraudulent transmission by verifying the validity of a transmission, message, station, or originator. During the process, the user enters a name or account number (identification) and password (authentication)

Authenticator: The material or credential used to create or implement authentication bindings such as a password, PIN number, token seed, smart card seed, etc.

Authorization: Granting the right of access to a user, program, or process. The privileges granted to an individual by a designated official to access data, based upon the individual's job, clearance, and/or need to know

Availability: The computer security characteristic that addresses requirements for IT systems and data to be operational in support of essential business functions and that measures the sensitivity of IT systems and data to unexpected outages

Backup: The process of producing a reserve copy of software or electronic files as a precaution in case the primary copy is damaged or lost.

Baseline Security Configuration: The minimum set of security controls that must be implemented on all IT systems of a particular type.

Business Function: A collection of related structural activities that produce something of value to the organization, its stakeholders or its customers. See also *Essential Business Function*.

Business Impact Analysis (BIA): The process of determining the potential consequences of a disruption or degradation of business functions

Chain of Custody: Documentation that is sufficient to prove continuous and unbroken possession of a confiscated IT system.

Change Control: A management process to provide control and traceability for all changes made to an application system or IT system.

Chief Information Officer of the Commonwealth (CIO): The CIO oversees the operation of the Virginia Information Technologies Agency (VITA) and, under the direction and control of the Virginia Information Technology Investment Board (the Board), exercises the powers and performs the duties conferred or imposed upon him by law and performs such other duties as may be required by the Board

Chief Information Security Officer of the Commonwealth (CISO): The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of COV IT systems and data

Commonwealth of Virginia (COV): The Executive Branch of the government of the Commonwealth of Virginia, or its Agencies or departments

Computer Emergency Response Team Coordination Center (CERT/CC): a center of Internet security expertise, located at the Software Engineering Institute at Carnegie Mellon University that studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to assist the CERTs of other organizations. See also *Incident Response Team* and *United States Computer Emergency Response Team (US-CERT)*.

Confidentiality. The computer security characteristic that addresses requirements that data is disclosed only to those authorized to access it, and that measures the sensitivity of data to unauthorized disclosure.

Configuration Management: A formal process for authorizing and tracking all changes to both hardware and software of an IT system during its life cycle, see also *Change Control*.

Continuity of Operations (COOP) Planning. The process of developing plans and procedures to continue the performance of essential business functions in the event of a business interruption or threat of interruption.

Continuity of Operations (COOP) Plan: A set of documented procedures developed to provide for the continuance of essential business functions during an emergency.

Control Objectives for Information and related Technology (COBIT): A framework of best practices (framework) for IT management that provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control.

Countermeasure. An action, device, procedure, technique, or other measure that reduces vulnerability or the impact of a threat to an IT system.

Credential: Information passed from one entity to another that is used to establish the sending entity's access rights.

Data: Data consists of a series of facts or statements that may have been collected, stored, processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information. Information can be processed and used to draw generalized conclusions or knowledge.

Database: A database is a collection of data organized into interrelated tables and specifications of data objects.

Data Classification: A process of categorizing data according to its sensitivity.

Data Communications: Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate Commonwealth of Virginia (COV) data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of this information. As used in this document, Data Communications is included in the definition of government database, herein.

Data Custodian. An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An Agency Division Director or Manager responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

Data Security: Data Security refers to those practices, technologies, and/or services used to apply security appropriately to data.

Disaster Recovery Plan (DRP): A set of documented procedures that identify the steps to restore essential business functions on a schedule that supports Agency mission requirements.

Data Storage Media. A device used to store IT data. Some examples of data storage media include floppy disks, fixed disks, CD-ROMs, and USB flash drives.

Encryption. A means of scrambling data so it cannot be read without the appropriate decryption methodology.

Essential Business Function. A business function is essential if disruption or degradation of the function prevents the Agency from performing its mission as described in the Agency mission statement.

Evaluation: Investigative and test procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific system weaknesses.

Extranet. A trusted network; used by COV to connect to a third-party provider.

Federal Information Security Management Act (FISMA): Federal legislation whose primary purpose is to provide a comprehensive framework for IT security controls in Federal agencies.

Firewall. Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted.

Function. A purpose, process, or role.

Government Database. For the purposes of this document, the term "government database" includes both databases that contain COV data and data communications that transport COV data. This definition applies irrespective of whether the COV information is in a physical database structure maintained by COV or a third-party provider. However, this definition does not include databases within Agencies that have been determined by the Agencies

themselves to be non-governmental. See also *Database* and *Data Communications*

Group: A named collection of IT system users; created for convenience when stating authorization policy.

Harden: The process of implementing software, hardware, or physical security controls to mitigate risk associated with COV infrastructure and/or sensitive IT systems and data

High Availability. A requirement that the IT system is continuously available, has a low threshold for down time, or both.

Identification. The process of associating a user with a unique user ID or logon ID.

Incident Response Capability (IRC): The follow-up to an unplanned event such as a hardware or software failure or attack against a computer or network

Incident Response Team (IRT): An organization within an Agency constituted to monitor IT security threats and prepare for and respond to cyber attacks. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *United States Computer Emergency Response Team (US-CERT)*

Individual Accountability. The process of associating one and only one IT system user or IT system (such as a workstation or terminal) with any actions performed.

Information Security Officer (ISO). The individual who is responsible for the development, implementation, oversight, and maintenance of the Agency's IT security program.

Information Technology (IT): Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services

Information Technology (IT) Infrastructure Library (ITIL): A framework of best practice processes designed to facilitate the delivery of high quality information technology (IT) services

Information Technology (IT) Security: The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality

Information Technology (IT) Security Architecture. The logical and physical security infrastructure made up of products, functions, locations, resources, protocols, formats, operational sequences, administrative and technical security controls, etc., designed to provide the appropriate level of protection for IT systems and data

Information Technology (IT) Security Audit. An independent review and examination of an IT system's policy, records, and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

Information Technology (IT) Security Auditor: CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or a private firm that, in the judgment of the Agency, has the experience and expertise required to perform IT security audits.

Information Technology (IT) Security Breach. The violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an IT system

Information Technology (IT) Security Controls. The protection mechanisms prescribed to meet the security requirements specified for an IT system. These mechanisms may include but are not necessarily limited to: hardware and software security features; operating procedures, authorization and accountability access and distribution practices; management constraints; personnel security; and environmental and physical safeguards, structures, and devices. Also called IT security safeguards and countermeasures

Information Technology (IT) Security Incident. An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an IT system. A security incident includes an attempt to violate an explicit or implied security policy.

Information Technology (IT) Security Logging: Chronological recording of system activities sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to its final results.

Information Technology (IT) Security Requirements. The types and levels of protection necessary to adequately secure an IT system

Information Technology (IT) Security Safeguards. See *Information Technology (IT) Security Controls*.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control See also *Application System* and *Support System*.

Information Technology (IT) System Users: As used in this document, a term that includes COV employees, contractors, vendors, third-party providers, and any other authorized users of COV IT systems, applications, telecommunication networks, data, and related resources It excludes customers whose only access is through publicly available services, such as public COV Web sites.

Insecure: Unprotected, as an IT system.

Integrity: The computer security characteristic that addresses the accuracy and completeness of IT systems and data, and that measures the sensitivity of IT systems and data to unauthorized or unexpected modification.

Integrity Check: Validates that a message has not been altered since it was generated by a legitimate source (based on representation of information as numbers and mathematic manipulation of those numbers).

Internet: An external worldwide public data network using Internet protocols to which the COV can establish connections. The COV has no control over the Internet and cannot guarantee the confidentiality, integrity, or availability of its communications.

Intranet: A trusted multi-function (data, voice, video, image, facsimile, etc) private digital network using Internet protocols, which can be developed, operated and maintained for the conduct of COV business

Intrusion Detection: A method of monitoring traffic on the network to detect break-ins or break-in attempts, either manually or via software expert systems.

Intrusion Detection Systems (IDS): Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack

Intrusion Prevention Systems (IPS): Software that prevents an attack on a network or computer system. An IPS is a significant step beyond an IDS (intrusion detection system), because it stops the attack from damaging or retrieving data. Whereas an IDS passively monitors traffic by sniffing packets off of a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

ISO/IEC 17799: An IT security standard published in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides best practice recommendations on IT security management for use by those who are responsible for initiating, implementing or maintaining information security management systems.

Key: A sequence of data used in cryptography to encrypt or decrypt information. The keys must be known or deduced to forge a digital signature or decrypt an encrypted message.

Key Escrow: The process of storing the encryption key with a third-party trustee to allow the recovery of encrypted text.

Least Privilege: The minimum level of data, functions, and capabilities necessary to perform a user's duties. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IT system.

Log: To record an action.

Log File: A chronological record of operational and security-related events that have occurred

Logon ID: An identification code (normally a group of numbers, letters, and/or special characters) assigned to a particular user that identifies the user to the IT system

Malicious Code: Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, damaging, or destroying IT systems and/or data. Malicious code includes viruses (boot sector, file infector, multipartite, link, stealth, macro, email, etc.), Trojan horses, trap doors, worms, spyware, malware, and counterfeit computer instructions (executables)

Malicious Software: See Malicious Code

Malware: A categeory of malicious software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.

Mission Critical Facilities: The data center's physical surroundings as well as data processing equipment inside and the systems supporting them that need to be secured to achieve the availability goals of the system function

Monitoring: Listening, viewing, or recording digital transmissions, electromagnetic radiation, sound, and visual signals.

Non-Sensitive Data: Data of which the compromise with respect to confidentiality, integrity, and/or availability could not adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled

Off-Site Storage: The process of storing vital records in a facility that is physically remote from the primary site. To qualify as off-site, the facility should be at least 500 yards from the primary site and offer environmental and physical access protection.

Operational Risk: Any risk that is not market risk or credit risk related. This includes the risk of loss from events related to technology and infrastructure failure, from business interruptions, from staff related problems and from external events such as regulatory changes. Examples of operational risk include: technology failure; business premises becoming unavailable; inadequate document retention or record-keeping; poor management; lack of supervision, accountability and control; errors in financial models and reports; attempts to conceal losses or make personal gains (rogue trading); and third-party fraud

Out-of-Band Communications: A way to send data (e.g., files) outside the context of normal communications. Out of band communications provide a secondary communications channel for emergencies and/or redundancy.

Password: A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Personal Digital Assistant (PDA). A digital device, which can include the functionality of a computer, a cellular telephone, a music player and/or a camera

Personal Identification Number (PIN). A short sequence of digits used as a password

Personnel. All COV employees, contractors, and subcontractors, both permanent and temporary

Phishing. A form of criminal activity characterized by attempts to acquire sensitive information fraudulently, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication

Plain Text Message. A message sent without encryption.

Privacy. The rights and desires of an individual to limit the disclosure of individual information

Privacy Officer: The privacy officer, if required by statute (such as HIPAA) provides guidance on the requirements of state and federal privacy laws; disclosure of and access to sensitive data; and security and protection requirements in conjunction with the IT system when there is some overlap among sensitivity, disclosure, privacy, and security issues.

Proprietary Information: Specific and unique material and information relating to or associated with a company's products, business, or activities. This information must have been developed for or by the company and must not be available freely from another source.

Recovery. Activities beyond the initial crisis period of an emergency or disaster that are designed to return IT systems and/or data to normal operating status.

Repudiation: Denial that one did or said something.

Residual Risk. The portion of risk that remains after security measures have been applied

Restoration: Activities designed to return damaged facilities and equipment to an operational status.

Restricted Data: Data which has limited availability; based on COV regulations

Risk. The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result

Risk Assessment (RA) and Management. The process of identifying the vulnerabilities, threats, likelihood of occurrence, potential loss or impact, and theoretical effectiveness of security measures. Results are used to evaluate the level of risk and to develop security requirements and specifications to manage the risk

Risk Mitigation. The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Roles and Responsibility: Roles represent a distinct set of operations and responsibilities required to perform some particular function that an individual may be assigned. Roles may differ from the individual's business title. This document contains the roles and responsibilities associated with implementing IT security

Recovery Time Objective (RTO). The amount of time targeted for the recovery of a business function or resource after a disaster occurs

Secure. A state that complies with the level of security controls that have been determined to provide adequate protection against adverse contingencies

Sensitive Data: Any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.

Sensitive IT Systems. COV IT systems that store, process, or transmit sensitive data

Sensitivity Classification. The process of determining whether and to what degree IT systems and data are sensitive.

Separation of Duties. Assignment of responsibilities such that no one individual or function has control of an entire process. Implied in this definition is the concept that no one person should have complete control. Separation of duties is a technique for maintaining and monitoring accountability and responsibility for IT systems and data

Shared Accounts. A logon ID or account utilized by more than one entity

Sign. The process of using a private key to generate a digital signature as a means of proving generation or approval of a message.

Signature. A quantity associated with a message that only someone with knowledge of a user's private key could have generated but which can be verified through knowledge of the user's public key

Spyware. A category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party

State: See *Commonwealth of Virginia (COV).*

Support System: An interconnected set of IT resources under the same direct management control that shares common functionality and provides services to other systems. See also *Application System* and *Information Technology (IT) System*

System. See *Information Technology (IT) System*

System Administrator. An analyst, engineer, or consultant who implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner. An Agency Division Director or Manager responsible for the operation and maintenance of an Agency IT system.

Third-Party Provider. A company or individual that supplies IT equipment, systems, or services to COV Agencies.

Threat. Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Token. A small tangible object that contains a built-in microprocessor utilized to store and process information for authentication.

Trojan horse. A malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. Trojan horse programs may look useful or interesting to an unsuspecting IT system user, but are actually harmful when executed.

Trusted. Recognized automatically as reliable, truthful, and accurate, without continual validation or testing.

United States Computer Emergency Response Team (US-CERT): A partnership between the Department of Homeland security and the public and private sectors, intended to coordinate the response to IT security threats from the Internet. As such it releases information about current IT security issues, vulnerabilities and exploits as Cyber Security Alerts, and works with software vendors to create patches for IT security vulnerabilities. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *Incident Response Team*.

Universal Serial Bus (USB). A standard for connecting devices.

Untrusted. Characterized by absence of trusted status. Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

USB Flash Drive. A small, lightweight, removable and rewritable data storage device (also commonly referred to as thumb drives, jump drives, etc.)

User ID. A unique symbol or character string that is used by an IT system to identify a specific user. See Logon ID.

Virginia Department of Emergency Management (VDEM): A COV department that protects the lives and property of Virginia's citizens from emergencies and disasters by coordinating the state's emergency preparedness, mitigation, response, and recovery efforts.

Version Control. A management process to traceability of updates to operating systems and supporting software.

Virus: See Malicious Code.

Virginia Information Technologies Agency (VITA): VITA is the consolidated, centralized IT organization for COV.

Vital Record. A document, regardless of media, which, if damaged or destroyed, would disrupt business operations.

Vulnerability: A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Workstation. A terminal, computer, or other discrete resource that allows personnel to access and use IT resources.

9. IT SECURITY ACRONYMS

AITR: Agency Information Technology Representative

ANSI: American National Standards Institute

BIA: Business Impact Analysis

CAP: Corrective Action Plan

CIO: Chief Information Officer

CISO: Chief Information Security Officer

COOP: Continuity of Operations Plan

COPPA: Children's Online Privacy Protection Act

COTS: Council on Technology Services

DHRM: Department of Human Resource Management

DMAS: Department of Medical Assistance Services

DRP: Disaster Recovery Plan

FIPS: Federal Information Processing Standards

FISMA: Federal Information Security Management Act

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

IRC: Incident Response Capability

ISA: Interconnection Security Agreement

ISO: Information Security Officer

IRT: Incident Response Team

ITRM: Information Technology Resource Management

MOU: Memorandum of Understanding

OMB: Office of Management and Budget

PDA: Personal Digital Assistant

PIA: Privacy Impact Assessment

PII: Personally Identifiable Information

PIN: Personal Identification Number

RA: Risk Assessment and Management

RBD: Risk-Based Decisions

RTO: Recovery Time Objective

SLA: Service Level Agreement

SDLC: Systems Development Life Cycle

SNMP: Simple Network Management Protocol

SOP: Standard Operating Procedure

SSID: Service Set Identifier

SSP: Security Program Plan

ST&E: Security Test & Evaluation

TSS: Technology Strategy and Solutions Directorate (VITA)

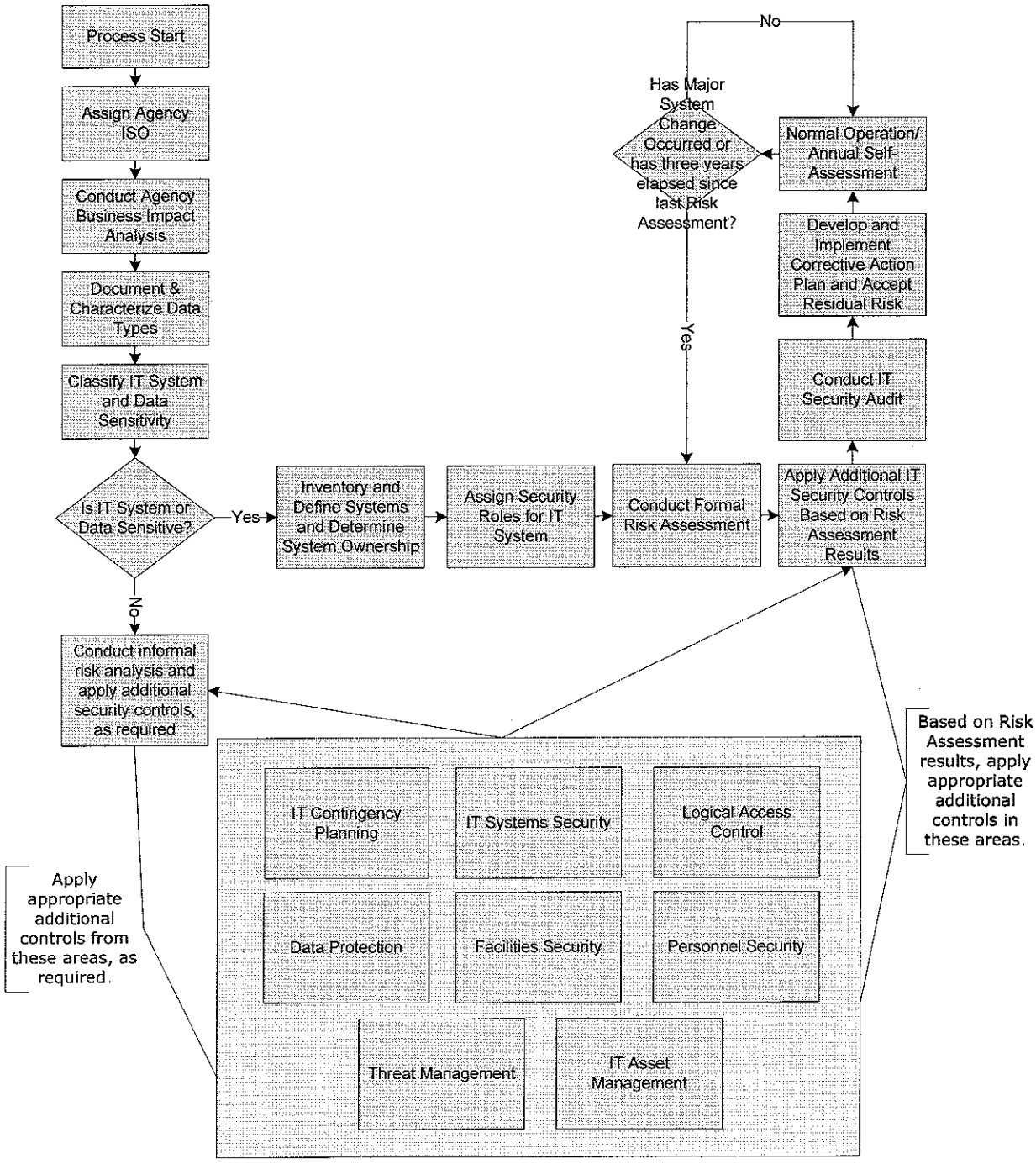
USCERT: Computer Emergency Response Team

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

APPENDIX 1

Appendix 1 below illustrates the process by which the DMAS IT Security Program components interact to enable DMAS to accomplish its mission in a safe and secure technology environment.



Appendix 1 – DMAS IT Security Framework

APPENDIX 2

COV Information Security Program

	COV IT Security Policy (SEC500-02)	Description
1	***Designate ISO for the Agency by 07/01/2007***	- via email from Agency Head to VITASecurityServices@vita virginia gov - include name, title & contact information - designate backup ISO if possible
2	***Inventory & Classify Agency IT Systems****	- identify all Agency IT systems - determine which Agency IT systems are sensitive (Confidentiality, Integrity, Availability) - determine appropriate level of protection for Agency IT systems (may rely on business impact analysis (BIA) performed for COOP)
3	***Perform Risk Assessment for Sensitive Agency IT Systems****	- define system boundaries on sensitive Agency IT systems - assess threats to sensitive Agency IT systems and data - apply the appropriate IT security controls necessary to reduce risks to an acceptable level
4	***Perform IT Security Audits on Sensitive IT Audit Systems***	- submit an audit plan for all sensitive Agency IT systems to VITA by 02/01/2007 - perform IT security audits periodically but not less than once every 3 years - prepare corrective action plans to address correct deficiencies
5	***Document & Exercise IT Contingency & DR plans****	- prepare COOP for the agency (per VDEM guidelines) including BIA - implement & document IT system backup and restore strategy - exercise IT disaster recovery components of COOP plan at least annually
6	***Implement IT Systems Security Standards****	- implement system configuration standards - implement protection against malicious code (virus) - implement security into IT Systems Development Life Cycle
7	***Document Account Management Practices****	- define measures to verify all IT system users - define user accounts based on least privilege practices - establish requirements for account management, passwords & remote access
8	***Define Data Protection Practices****	- establish requirements for protection on laptops and mobile media - implement security safeguards for processing and storing of data
9	***Safeguard Physical Facilities****	- ensure servers & network equipment are in a secure location - provide for environmental conditions to protect equipment and interruption to computer services
10	***Establish Security Awareness Training Program & Acceptable Use Policies***	- implement Security Awareness Training Program for all IT users, including contractors - include training on Acceptable Use policy as part of Security Awareness Training
11	***Report & Respond to IT Security Incidents***	- implement process to detect & respond to IT security incidents - report IT security incidents to CIO within 24 hours (2.2-603.F) - perform IT security monitoring & logging on systems
12	***Implement IT Asset Controls****	- implement IT asset inventory & control- implement process for software license management- implement configuration management and change control
Note: *	**For agencies receiving infrastructure services from VITA, these areas will require coordination with VITA to document.** **Requests can be made through the agency CAM**	

APPENDIX 3 – IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM

If a DMAS Division Director has a need to request an exception to any requirement of this policy and the related Standards, the exception must be submitted using the form on the following page.

Department of Medical Assistance Services
IT Security Policy & Standard Exception Request Form

Date of Request: _____

Requester: _____ **Agency Name:** _____

IT Security Policy or Standard to which an exception is requested:

_____

In each case, the Division requesting the exception must

1. Provide the **Business or Technical Justification** for not implementing the Policy or Standard:

2. Describe the scope and extent of the exception (and attach detailed information as needed):

3. Identify the safeguards to be implemented to mitigate risks associated with the exception:

4. Define the specific duration of the exception (not to exceed six (6) months):

Approved _____ _____
Agency Head Date

DMAS Information Security Officer (ISO) or backup ISO Use Only

Recommend: Approval_____ Denial_____ Comments:

_____ _____
DMAS ISO or backup ISO Date

DMAS Security Advisory Committee Use Only

Recommend: Approval:_____ Denial: _____ Comments:

_____ _____
DMAS Security Advisory Committee Chair Date

DMAS Agency Head Use Only

Recommend: Approval:_____ Denial: _____ Comments:

_____ _____
DMAS Agency Head Date

Department of Medical Assistance Services
IT Security Policy & Standard Exception Request Form

Appeal: An appeal must go through the same channels as before for a second review before a final decision is made.

(Repeat Page 1 of this form above along with this second page for a second review consideration).

DMAS Security Advisory Committee Use Only

Recommend: Approval:_____ Denial: _____ Comments:

_____ _____
DMAS Security Advisory Committee Chair Date

DMAS Agency Head Use Only

Recommend: Approval:_____ Denial: _____ Comments:

_____ _____
DMAS Agency Head Date

Commonwealth of Virginia

Department of Medical Assistance Services

Office of Compliance and Security

HIPAA Security Policies

Authorized on May 21, 2007

This page left intentionally blank

Table of Contents

Introduction

This document contains the HIPAA Security Policies for the Department of Medical Assistance Services (DMAS). The DMAS Office of Compliance and Security (OCS), with the support of security staff in the DMAS Information Management Division have developed these policies pursuant to the requirements in 45 CFR Parts 160, 162, and 164 Health and Insurance Reform: Security Standards: Final Rule February 20, 2003.

Security and privacy are inextricably linked. The Privacy Rule sets standards for how protected health information (PHI) should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information. The protection of the privacy of information depends in large part on the existence of security measures to protect that information.

The security standards define administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (PHI). The standards require covered entities such as DMAS to implement basic safeguards to protect PHI from unauthorized access, alteration, deletion, and transmission.

Procedures to implement the provisions of these policies will be developed in consideration of industry best practices noted in *A Review of Information Security in the Commonwealth of Virginia*, Auditor of Public Accounts, dated December 1, 2006.

Ethics

Ethics - The safety of the Commonwealth, duty to our principals, and to each other requires that we adhere to, and be seen to adhere to, the highest ethical standards of behavior. Staff in the OCS will:

- Protect society, the Commonwealth, and the infrastructure;
- Act honorably, honestly, justly, responsibly, and legally;
- Provide diligent and competent service to principals; and
- Advance and protect the profession.
- Discourage such behavior as:
    - Raising unnecessary alarm, fear, uncertainty, or doubt
    - Giving unwarranted comfort or reassurance
    - Consenting to bad practice
    - Attaching weak systems to the public network
    - Professional association with non-professionals
    - Professional recognition of, or association with amateurs
    - Associating or appearing to associate with criminals or criminal behavior.[1]

[1]Adapted from Code of Ethics, International Information Systems Security Certification Consortium (ISC)²

Policy, Standards, Baselines, Guidelines and Procedures

Policy

Security Policy is defined as a broad statement of principles that represents management's view for a defined control area. Security policy is strategic and dictates the role security has in DMAS. Security policies may be organizational, issue-specific or system specific.

1. Organizational security policy – how the security program will be set up, establishes security programs goals, assigns responsibilities, illustrates strategic and tactical value of security, identifies/outlines enforcement procedures, addresses, relevant laws, regulations and liability issues and provides scope and direction for all current and future security-related activities within DMAS and describes the amount of risk DMAS is willing to take.

2. Issue-specific policies – functional implementing policies that address specific security issues felt to need more detailed explanation and attention to ensure a comprehensive structure is built and, that all employees are aware and understand how they are to comply.

3. System-specific policies – presents management decisions that are closer to the actual computers, networks, applications, and information and key assets.

Additionally, DMAS policy may fall into one of the following categories:

1. Regulatory – written to ensure the organization is following standards set by specific law(s).

2. Advisory – written to suggest certain types of behaviors and activities should take place and outlines the sanctions if employees do not comply.

3. Informative – written to inform employees of certain topics; not necessarily an enforceable policy, but designed to teach about specific issues.

Standards

Standards are rules that specify how security technology (hardware and software products) will be used and dictate a particular course of action or response to a given situation. Standards are mandatory.

Baseline

Baseline is a platform-specific security rule, accepted as providing the most effective approach to a security implementation.

Procedures

Procedures define specifically how policy, standards, baselines and guidelines will be implemented in a given situation. DMAS has adopted a procedures template included in Appendix A.

Guidelines

Guidelines are general statements, used to recommend or suggest an approach to implementation of: policy, standards and baselines.[2]

[2] Chris Hare, CISSP, CISA, "Policy Development" Information Security Management Handbook, 5th Edition, 2004, pp 925 - 943

Security Rule Background

"The Security Rule's requirements are organized into three categories: *administrative safeguards*, *physical safeguards*, and *technical safeguards*. Within these three categories are 18 standards, 12 of which have implementation specifications, six of which do not. A *standard* defines what a Covered Entity (CE) must do; *implementation specifications* describe how it must be done. The Security Rule has 36 implementation specifications, which are further divided into two types: required (14) and addressable (22). Required specifications are critical and CEs must implement them. CEs have three choices, however, for handling addressable implementation specifications:

1. If a specific addressable implementation specification is determined to be reasonable and appropriate, the CE must implement it.
2. If implementing a specific addressable implementation specification is not reasonable and appropriate, but the overall standard *cannot* be met without an additional security measure, a CE must:
    a. Document why it would not be reasonable and appropriate to implement the implementation specification; and
    b. Implement and document the alternative security measure that accomplishes the same purpose as the addressable implementation specification.
3. If implementing a specific addressable implementation specification is not reasonable and appropriate, but the overall standard *can* be met without implementation of an alternative security measure, a CE must document:
    a. The decision not to implement the addressable specification
    b. Why it would not be reasonable and appropriate to implement the implementation specification; and
    c. How the standard is being met."

Administrative safeguards

Administrative safeguards make up 50% of the Security Rule's standards. They require documented policies and procedures for managing day-to-day operations, the conduct and access of workforce members to electronic protected health information (EPHI), and the selection, development, and use of security controls. The specific standards of the administrative safeguards are:

Security management process	An overall requirement to implement policies and procedures to prevent, detect, contain, and correct security violations.
Assigned security responsibility	A single individual must be designated as having overall responsibility for the security of a CE's EPHI.
Workforce security	Policies, procedures, and processes must be developed and implemented that ensure only properly-authorized workforce members have access to EPHI.
Information access management	Policies, procedures, and processes must be developed and implemented for authorizing, establishing, and modifying access to EPHI.
Security awareness and training	A security awareness and training program for a CE's entire workforce must be developed and implemented.
Security incident procedures	Policies, procedures, and processes must be developed and implemented for reporting, responding to, and managing security incidents.
Contingency plan	Policies, procedures, and processes must be developed and implemented for responding to a disaster or emergency that damages information systems containing EPHI.
Evaluation	CEs must perform periodic technical and non-technical evaluations that determine the extent to which a CE's security policies, procedures, and processes meet the ongoing requirements of the Security Rule.
Business associate contracts and other arrangements	CEs must -- when dealing with business associates that create, receive, maintain, or transmit PHI on the CE's behalf -- develop and implement contracts that ensure the business associate will appropriately safeguard the information.

Physical safeguards

The physical safeguards are a series of requirements meant to protect a CE's electronic information systems and PHI from unauthorized physical access. CE's must limit physical access while permitting properly-authorized access. The specific standards are:

Facility access controls	An overall requirement to implement policies, procedures, and processes that limit physical access to electronic information systems while ensuring that properly-authorized access is allowed.
Workstation use	Policies and procedures must be developed and implemented that specify appropriate use of workstations and the characteristics of the physical environment of workstations that can access EPHI.
Workstation security	CE's must implement physical safeguards for all workstations that can access EPHI in order to limit access to only authorized users.
Device and media controls	Policies, procedures, and processes must be developed and implemented for the receipt and removal of hardware and electronic media that contain EPHI into and out of a CE, and the movement of those items within a CE.

Technical safeguards

The technical safeguards are several requirements for using technology to protect EPHI, particularly controlling access to it. The specific standards are:

Access control	Policies, procedures, and processes must be developed and implemented for electronic information systems that contain EPHI to only allow access to persons or software programs that have appropriate access rights.
Audit controls	Mechanisms must be implemented to record and examine activity in information systems that contain or use EPHI.
Integrity	Policies, procedures, and processes must be developed and implemented that protect PHI from improper modification or destruction.
Person or entity authentication	Policies, procedures, and processes must be developed and implemented that verify persons or entities seeking access to EPHI are who or what they claim to be.
Transmission security	Policies, procedures, and processes must be developed and implemented that prevent unauthorized access to EPHI that is being transmitted over an electronic communications network (e.g., the Internet).

Documentation Standard

CE's must maintain all documentation (e.g., policies, procedures) required by the Security Rule for a period of six years from the date of its creation or the date when it last was in effect, whichever is later. Such documentation must be made available to the workforce members responsible for implementing the policies and procedures. Additionally, CE's must periodically review such documentation and revise and update it as needed to ensure the confidentiality, integrity, and availability of EPHI."[3]

[3] Steven Weil, CISSP, CISA, CBCP "HIPAA Security Rule" 2004-03-02 http://www.securityfocus.com/infocus/1764

Precedence of HIPAA Security vs. Information Security Policies

DMAS must comply with both the Federal HIPAA Security Rule and the Commonwealth of Virginia Information Technology Agency (VITA) Policies and Standards. In the event of a conflict between DMAS HIPAA Security Policies, developed to comply with the HIPAA Security Rule, and DMAS Information Security Policies, developed to comply with VITA requirements, the more stringent policy will apply.

Precedence of HIPAA Security vs. HIPAA Privacy Policies

The DMAS HIPAA Privacy Policies, developed prior to the finalization of the HIPAA Security Rule, were under review when these policies were authorized. Pending final review and updates to the HIPAA Privacy Policies, in the event of a conflict between DMAS HIPAA Security Policies, developed to comply with the HIPAA Security Rule, and DMAS HIPAA Security Policies, developed to comply with then current requirements, the more stringent policy will apply.

Scope of HIPAA Security Policies

These policies are applicable to the DMAS workforce and all DMAS Divisions that use or disclose PHI for any purposes.

DMAS Staff Responsibilities

DMAS Director and Executive Management Team - DMAS Director and Executive Management Team are responsible for ensuring the confidentiality, integrity and availability of PHI contained on DMAS information systems by *authorizing* the implementation of appropriate and reasonable security policies, procedures and controls.

DMAS Security Advisory Committee (SAC) - The responsibilities of the SAC include but are not limited to:

- Reviewing and approving DMAS information security policies.
- Approving and supporting DMAS security awareness and training programs.
- Approving and supporting the DMAS information security sanction policy.

Human Resources Division - The DMAS Human Resources Division is responsible for ensuring that appropriate pre-hire clearance activities are conducted (e.g., background checking, references, credit checks, etc.,) and for coordinating with the Office of Compliance and Security to ensure the mandatory HIPAA Training course is completed before a workforce member is allowed access to DMAS information systems containing PHI.

Information Management (IM) Division – IM is responsible for implementing technical security solutions and documenting all related security procedures. IM is also responsible for creating and maintaining the Contingency Plan for inclusion in the DMAS Continuity of Operations (COOP) Plan that is managed and maintained by the Office of Compliance and Security.

Office of Compliance and Security (OCS) – OCS is responsible for security governance and oversight of the overall DMAS security program. OCS provides advice and guidance to other Divisions, creates policy and awareness training, and periodically reviews security operations. OCS is responsible for the planning and oversight of a comprehensive privacy, information and physical security program for the Department, to include:

- Information Security Officer (ISO) functions related to the security of all DMAS information in whatever form or media to comply with all security policies and standards of the Virginia Information Technologies Agency (VITA);
- HIPAA compliance through management of the OCS Privacy Office;
- Management of the Department's Continuity of Operations (COOP) Plan; Compliance with the DMAS Code of Ethics and Business Conduct;
- Serving as the Chairperson for the Security Advisory Committee; and
- Risk management in compliance with VITA's Information Technology Risk Management Guidelines SEC 506-01 dated 12/11/06 and the HIPAA Security Rule standard of §164.308(a)(1)(ii)(B).

DMAS Division Directors - Division Directors are responsible for ensuring Divisional compliance with security policies and awareness training as mandated, participating in OCS-sponsored security training and periodic meetings as applicable, ensuring that their staff annually review and complete the web-based Security Awareness Training, and ensuring that complete participation in OCS-sponsored security training is achieved within their departments.

DMAS workforce members who create PHI are responsible for including but are not limited to:

- Understanding the data for which they are responsible and ensuring its confidentiality, integrity and availability.
- Specifying and approving the use of security policies, procedures and controls for the PHI for which they are responsible.
- Authorizing appropriate access to PHI for which they are responsible.
- Promptly reporting security violations and risks to the PHI for which they are responsible.
- Assisting in investigations of security violations with respect to the PHI for which they are responsible.
- Promoting DMAS security training and awareness for all workforce members.

DMAS data custodians are providers of data processing services such as application software, networks, operating systems, etc. The responsibilities of DMAS data custodians include but are not limited to:

- Administering security policies, procedures and controls.
- Coordinating the identification of DMAS data processing assets.
- Ensuring the effective use of data backup procedures for DMAS' information systems containing PHI.
- Ensuring the confidentiality, integrity and availability of DMAS data network and information system operating systems.
- Maintaining the confidentiality of all data processed, handled, or seen in the performance of data custodian duties.
- Ensuring there is appropriate supervision of workforce members performing maintenance activities on DMAS information systems containing PHI.

DMAS data users are users of DMAS data processing services such as application software and data, networks, operating systems, etc. The responsibilities of DMAS data users include but are not limited to:

- Using DMAS data processing resources only for intended purposes.
- Promoting awareness and use of DMAS security controls.
- Complying with all appropriate DMAS HIPAA, DMAS Information Security, and VITA Information Security policies, procedures and standards.
- Promptly reporting security violations.
- Attending appropriate DMAS security training and awareness.

All DMAS workforce members are responsible for appropriately safeguarding protected health information (PHI) contained on DMAS information systems from unauthorized access, modification, destruction and disclosure.

Compliance with DMAS and State Policies

All DMAS workforce members must comply with DMAS written policies. Failure to comply with written policy may result in disciplinary action under the Standards of Conduct, Policy No : 1.60, of the Virginia Department of Human Resource Management.

Review of DMAS Policies

All HIPAA Security policies will be reviewed annually to determine if the policy complies with current HIPAA Security regulations. In the event that significant related regulatory changes occur, the policy will be updated as needed.

THIS PAGE INTENTIONALLY LEFT BLANK

Policies on the Standards for Administrative Safeguards

THIS PAGE INTENTIONALLY LEFT BLANK

Security Management Process

HIPAA Security Rule Language: *Implement policies and procedures to prevent, detect, contain, and correct security violations.*

Purpose: This policy reflects DMAS' commitment to ensure the confidentiality, integrity, and availability of its information systems containing PHI by implementing policies and procedures to prevent, detect, contain, and correct security violations.

Policy: DMAS will ensure the confidentiality, integrity, and availability of its information systems containing PHI by implementing appropriate and reasonable policies, procedures and controls to prevent, detect, contain, and correct security violations. At a minimum, DMAS' security management process will include the following:

1. DMAS management's commitment to ensure the confidentiality, integrity, and availability of its information systems containing PHI.

2. Security policies, procedures and controls that reasonably and appropriately mitigate identified risks to DMAS information systems containing PHI and regular review and revision, as necessary, of such security policies, procedures and controls.

3. Regular training and awareness of DMAS workforce members on such security policies, procedures and controls.

4. DMAS' security management process will be based on formal and regular risk analysis and management.

Reference: 45 CFR 164.308(a)(1)(i) (Required)

Related Policies:
Risk Analysis
Risk Management
Information System Activity Review
Sanction Policy

Risk Analysis

HIPAA Security Rule Language: *Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (PHI) held by the covered entity.*

Purpose: This policy reflects DMAS' commitment to regularly conduct accurate and thorough analysis of the potential risks to the confidentiality, integrity, and availability of its information systems containing PHI.

Policy:

1. DMAS will regularly identify, define and prioritize risks to the confidentiality, integrity, and availability of its information systems containing PHI.

2. The identification, definition and prioritization of risks to DMAS information systems containing PHI must be based on a formal, documented risk analysis process. At a minimum, DMAS' risk analysis process must include the following:
   - Identification and prioritization of the threats to DMAS information systems containing PHI.
   - Identification and prioritization of the vulnerabilities of DMAS information systems containing PHI.
   - Identification and definition of security measures used to protect the confidentiality, integrity, and availability of DMAS information systems containing PHI.
   - Identification of the likelihood that a given threat will exploit a specific vulnerability on a DMAS information system containing PHI.
   - Identification of the potential impacts to the confidentiality, integrity, and availability of DMAS information systems containing PHI if a given threat exploits a specific vulnerability.

3. DMAS will conduct a risk analysis on a regular basis. Such risk analysis must be used in conjunction with DMAS' risk management process to identify, select and implement security measures to protect the confidentiality, integrity, and availability of DMAS information systems containing PHI. When possible, DMAS' risk analysis process should use both qualitative and quantitative data. Judgments used in DMAS' risk analysis, such as assumptions, defaults, and uncertainties, should be explicitly stated and documented.

4. DMAS will conduct a risk analysis when environmental or operational changes occur which significantly impact the confidentiality, integrity or availability of specific information systems containing PHI. Such changes include, but are not limited to:
   - Significant security incidents to specific DMAS information systems containing PHI.
   - Significant new threats or risks to specific DMAS information systems containing PHI.
   - Significant changes to the organizational or technical infrastructure of DMAS which affect specific DMAS information systems containing PHI.
   - Significant changes to DMAS information security requirements or responsibilities which affect specific DMAS information systems containing PHI.

5. DMAS risk analysis process will be based on the following steps:

- **Inventory**. DMAS will conduct a regular inventory of its information systems containing PHI and the security measures protecting those systems.
- **Threat identification.** DMAS will identify all potential threats to its information systems containing PHI. Such threats may be natural, human or environmental.
- **Vulnerability identification**. DMAS will identify all vulnerabilities on its information systems containing PHI. This should be done by regularly reviewing vulnerability sources and performing security assessments.
- **Security control analysis**. DMAS will analyze the security measures that have been implemented or will be implemented to protect its information systems containing PHI; this includes both preventive and detective controls.
- **Risk likelihood determination**. DMAS will assign ratings to specific risks that indicate the probability that vulnerability will be exploited by a particular threat. Three factors should be considered: 1) threat motivation and capability, 2) type of vulnerability, and 3) existence and effectiveness of current security controls
- **Impact analysis**. DMAS will determine the impact to confidentiality, integrity or availability that would result if a threat were to successfully exploit vulnerability on a DMAS information system containing PHI.
- **Risk Determination**. DMAS will use the information obtained in the above six steps to identify the level of risk to specific information systems containing PHI. For each vulnerability and associated possible threat, DMAS will make a risk determination based on:
  - The likelihood a certain threat will attempt to exploit a specific vulnerability.
  - The level of impact should the threat successfully exploit the vulnerability.
  - The adequacy of planned or existing security controls.

The results of each of the above steps must be formally documented and securely maintained.

Reference: 45 CFR 164.308(a)(1)(ii)(A) (Required)

Related Policies: Sanction Policy
Risk Management
Information System Activity Review
Security Management Process

Risk Management

HIPAA Security Rule Language: *Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec. 164.306 (a).*

Purpose: This policy reflects DMAS' commitment to select and implement security measures to reduce the risks to its information systems containing PHI to a reasonable and appropriate level.

Policy:

1. DMAS will implement security measures that reduce the risks to its information systems containing PHI to reasonable and appropriate levels.

2. Selection and implementation of such security measures will be based on a formal, documented risk management process. At a minimum, DMAS' risk management process will include the following:
   - Assessment and prioritization of risks to DMAS information systems containing PHI.
   - Selection and implementation of reasonable, appropriate and cost-effective security measures to manage, mitigate, or accept identified risks.
   - DMAS workforce member training and awareness on implemented security measures.
   - Regular evaluation and revision, as necessary, of DMAS' security measures.

3. DMAS will manage risk on a continuous basis and all selected and implemented security measures will ensure the confidentiality, integrity and availability of DMAS information systems containing PHI. Strategies for managing risk should be commensurate with the risks to such systems. One or more of the following methods may be used to manage risk:
   - Risk acceptance
   - Risk avoidance
   - Risk limitation
   - Risk transference

4. DMAS' risk management process will be based on the following steps:
   - **Inventory.** DMAS will conduct a regular inventory of its information systems containing PHI and the security measures protecting those systems. DMAS will be able to identify its information systems and the relative value and importance of those systems.
   - **Risk prioritization.** Based on the risks defined by DMAS' risk analysis, risks will be prioritized on a scale from high to low based on the potential impact to information systems containing PHI and the probability of occurrence. When deciding what DMAS resources should be allocated to identified risks, highest priority will be given to those risks with unacceptably high risk rankings.
   - **Method selection.** DMAS will select the most appropriate security methods to minimize or eliminate identified risks to DMAS information systems containing PHI. Such selections will be based on the nature of a specific risk and the feasibility and effectiveness of a specific method.
   - **Cost-benefit analysis.** DMAS will identify and define the costs and benefits of implementing or not implementing specific security methods.

- **Security method selection**. Based on its cost-benefit analysis, DMAS will determine the most appropriate, reasonable and cost-effective security method(s) for reducing identified risks to DMAS information systems containing PHI.
- **Assignment of responsibility.** DMAS workforce members who have the appropriate expertise will be identified and assigned responsibility for implementing selected security method(s).
- **Security method implementation**. Selected security method(s) will be correctly implemented.
- **Security method evaluation**. Selected security method(s) will be regularly evaluated and revised as necessary.

Reference: 45 CFR 164.308(a)(1)(ii)(B) (Required)

Related Policies: Risk Analysis
Sanction Policy
Information System Activity Review
Security Management Process

Sanction

HIPAA Security Rule Language: *Apply appropriate sanctions against DMAS workforce members who fail to comply with the security policies and procedures of the covered entity*

Purpose: This policy reflects DMAS' commitment to apply appropriate sanctions against DMAS workforce members who fail to comply with its security policies and procedures.

Policy:

1. DMAS workforce members must comply with all applicable DMAS security policies and procedures to ensure the confidentiality, integrity and availability of DMAS information systems.

2. DMAS workforce members must understand and be aware of all applicable DMAS security policies and procedures. DMAS must provide regular training and awareness for workforce members on DMAS security policies and procedures.

3. DMAS must have a formal, documented process for applying appropriate sanctions against workforce members who do not comply with its security policies and procedures. At a minimum, the process must include:
   - Procedures for detecting and reporting workforce members' non-compliance with DMAS security policies and procedures.
   - Identification and definition of levels of sanctions, including their relative severity.
   - Identification of cause and rationale for issuing of sanction and a defined, formal method for evaluating the severity of non-compliance with DMAS security polices and procedures.

4. Sanctions must be commensurate with the severity of the non-compliance with DMAS security polices and procedures.

5. The identification and definition of such sanctions must occur with appropriate involvement of DMAS' Human Resources Division and the Office of Compliance and Security.

6. Sanctions, administered in accordance with the Standards of Conduct, may include but are not limited to:
   - Suspension
   - Required retraining
   - Letter of reprimand
   - Termination

Reference: 45 CFR 164.308(a)(1)(ii)(C) (Required)

Related Policies: Risk Analysis
Risk Management
Information System Activity Review
Security Management Process

Information System Activity Review

HIPAA Security Rule Language: *Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*

Purpose: This policy reflects DMAS' commitment to regularly review records of activity on information systems containing PHI.

Policy:

1. DMAS will regularly review records of activity on information systems containing PHI. Records of activity may include but are not limited to:
   - Audit logs
   - Access reports
   - Security incident tracking reports

2. Appropriate hardware, software, or procedural auditing mechanisms will be implemented on DMAS information systems that contain or use PHI. At a minimum, such mechanisms must provide the following information:
   - Date and time of activity
   - Origin of activity
   - Identification of user performing activity
   - Description of attempted or completed activity

3. The level and type of auditing mechanisms that must be implemented on DMAS information systems that contain or use PHI must be determined by DMAS' risk analysis process. Auditable events may include but are not limited to:
   - Access to sensitive data
   - Use of audit software programs or utilities
   - Use of a privileged account
   - Information system start-up or stop
   - Failed authentication attempts
   - Security incidents

4. Records of activity created by audit mechanisms implemented on DMAS information systems will be reviewed regularly. The frequency of such review will be determined by DMAS' risk analysis. At a minimum, the risk analysis must consider the following factors:
   - The importance of the applications operating on the information system
   - The value or sensitivity of the data on the information system
   - The extent to which the information system is connected to other information systems

5. Such review must be via a formal documented process. At a minimum, the process must include:
   - Definition of which workforce members will review records of activity
   - Definition of what activity is significant
   - Definition of which activity records need to be archived and for what period of time
   - Procedures defining how significant activity will be identified and reported

- Procedures for preserving records of significant activity

6. Whenever possible, DMAS workforce members should not monitor or review activity related to their own user account.

Reference: 45 CFR 164.308(a)(1)(ii)(D) (Required)

Related Policies:
Security Management Process
Risk Analysis
Risk Management
Sanction
Audit Controls, Security Incident Procedures
Response and Reporting

Assigned Security Responsibility

HIPAA Security Rule Language: *Identify the security official who is responsible for the development and implementation of the policies required by this subpart for the covered entity.*

Purpose: This policy reflects DMAS' commitment to assign a single employee overall final responsibility for the confidentiality, integrity, and availability of its PHI.

Policy:

1. One function of the DMAS Office of Compliance and Security is to ensure the confidentiality, integrity, and availability of DMAS information systems and PHI. DMAS' Compliance and Security Officer leads this office and is responsible for the development and implementation of all policies necessary to appropriately protect the confidentiality, integrity, and availability of DMAS information systems and PHI.

2. The DMAS Compliance and Security Officer's responsibilities include, but are not limited to:
   - Ensure that DMAS information systems comply with all applicable federal, state, and local laws and regulations.
   - Ensure that no DMAS information system compromises the confidentiality, integrity, or availability of any other DMAS information system.
   - Develop, document, and ensure dissemination of appropriate security policies for the users and administrators of DMAS information systems and the data contained within them.
   - Ensure that newly acquired DMAS information systems have features that support required and/or addressable security Implementation Specifications.
   - Coordinate the selection, implementation, and administration of significant DMAS security controls.
   - Ensure DMAS workforce members receive regular security awareness training.
   - Conduct periodic risk analysis of DMAS information systems and security processes.
   - Develop and implement an effective risk management program.
   - Regularly monitor and evaluate threats and risks to DMAS information systems.
   - Monitor records of DMAS information systems' activity to identify inappropriate activity.
   - Ensure that an inventory of all DMAS information systems that contain PHI is maintained.
   - Create an effective security incident response policy and oversee related procedures.
   - Ensure adequate physical security controls exist to protect DMAS' PHI.
   - Coordinate with DMAS' Privacy Officer to ensure that security policies, procedures and controls support compliance with the HIPAA Privacy Rule.
   - Evaluate new security technologies that may be appropriate for protecting DMAS' information systems.

Reference: 45 CFR 164.308(a)(2)(i) (Required)

Related Policies: DMAS Information Security Policy

Workforce Security

HIPAA Security Rule Language: *Implement policies and procedures to ensure that all members of workforce have appropriate access to PHI and to prevent those workforce members who do not need to have access to PHI from obtaining access to PHI.*

Purpose: This policy reflects DMAS' commitment to allow access to information systems containing PHI only to workforce members who have been appropriately authorized. The type and extent of access authorized to DMAS information systems containing PHI must be based on risk analysis.

Policy:

1. DMAS will protect the confidentiality, integrity, and availability of its information systems containing PHI by preventing unauthorized access while ensuring that properly authorized workforce member access is allowed.

2. Access to DMAS information systems containing PHI will be granted to only to workforce members who have been properly authorized.

3. The type and extent of access to DMAS information systems containing PHI will be based on risk analysis.

4. Access to DMAS information systems containing PHI will be authorized only for properly trained DMAS workforce members having a legitimate need for specific information in order to accomplish job responsibilities. All such access must be defined and documented. Such access must be regularly reviewed and revised as necessary.

5. Access to DMAS information systems containing PHI will be established via a formal, documented process. At a minimum, this process must include:
   - Identification and definition of permitted access methods
   - Identification and definition of how long access will be granted to user
   - Procedure for granting a workforce member an access method (e.g., password or token) or changing an existing access method
   - Procedure for managing access rights in a distributed and networked environment
   - Appropriate tracking and logging of actions by authorized workforce members on DMAS information systems containing PHI
   - Procedures for limiting the number of accounts per user per application

6. DMAS workforce members must not attempt to gain access to DMAS information systems containing PHI for which they have not been given proper authorization.

7. As defined in DMAS' **Authorization and/or Supervision policy**, DMAS will ensure that all workforce members who have the ability to access DMAS information systems containing PHI are appropriately authorized or supervised.

8. As defined in DMAS' **Workforce Clearance policy**, DMAS workforce members must be adequately screened during the hiring process, including background checks as appropriate.

9. As defined in DMAS' **Termination Procedures policy**, DMAS must create and implement a formal, documented process for terminating access to PHI when the employment of a workforce member ends.

Reference: 45 CFR 164 308(a)(3)(i) (Addressable)

Related Policies:
Authorization and/or Supervision
Workforce Clearance Procedure
Termination Procedures
Access Control
Information Access Management
Access Authorization
Access Establishment and Modification
Facility Access Controls

Authorization and/or supervision

HIPAA Security Rule Language: *Implement procedures for the authorization and/or supervision of DMAS workforce members who work with PHI or in locations where it might be accessed.*

Purpose: This policy reflects DMAS' commitment to ensure that all workforce members who can access DMAS information systems containing PHI are appropriately authorized or supervised.

Policy:

1. DMAS will ensure that all workforce members who can access DMAS information systems containing PHI are appropriately authorized to access the system or supervised when they do so.

2. DMAS will have a formal documented process for authorizing appropriate access to DMAS information systems containing PHI. At a minimum, the process must include:
   - Procedure for granting different levels of access to DMAS information systems containing PHI.
   - Procedure for tracking and logging authorization of access to DMAS information systems containing PHI.
   - Procedure for regularly reviewing and revising, as necessary, authorization of access to DMAS information systems containing PHI.

3. DMAS workforce members must not be allowed access to information systems containing PHI until properly trained (i.e., Mandatory HIPAA Security Awareness Training) and authorized.

4. The type and extent of access granted to DMAS information systems containing PHI will be based on risk analysis.

5. Appropriate DMAS information system owners or their chosen delegates must define and authorize all access to DMAS information systems containing PHI. Such information system owners and delegates must be formally designated and documented.

6. Access to DMAS information systems containing PHI must be granted only for DMAS workforce members who have a need for specific PHI in order to accomplish a legitimate task. All such access must be defined and documented. Such access must also be regularly reviewed and revised as necessary.

7. DMAS workforce members must not attempt to gain access to DMAS information systems containing PHI for which they have not been given proper authorization.

8. DMAS will ensure that the confidentiality, integrity, and availability of PHI on DMAS information systems is maintained when its information systems are accessed by third parties.

9. Before third party persons are granted access to DMAS information systems containing PHI or DMAS locations where PHI can be accessed, a risk analysis must be performed.

10. Access by third party persons to DMAS information systems containing PHI or DMAS locations where PHI can be accessed must be allowed only after appropriate security controls have been implemented and a Business Associate agreement (BAA) has been signed defining the terms for access. The agreement must define the following:

- The security processes and controls necessary to ensure compliance with DMAS' security policies.
- Restrictions regarding the use and disclosure of DMAS data.
- DMAS' right to monitor and revoke third party persons' access and activity.

11. Where appropriate, third party persons should be supervised by an appropriate DMAS employee when they are accessing DMAS information systems containing PHI or in a DMAS location where PHI might be accessed.

Reference: 45 CFR 164.308(a)(3)(ii)(A) (Addressable)

Related Policies: Workforce Security
Workforce Clearance Procedure
Termination Procedures
Access Authorization

Workforce Clearance Procedure

HIPAA Security Rule Language: *Implement procedures to determine that the access of a workforce member to PHI is appropriate*

Purpose: This policy reflects DMAS' commitment to ensure that all workforce members have appropriate authorization to access DMAS information systems containing PHI.

Policy:

1. The background of all DMAS' workforce members must be adequately reviewed during the hiring process. Verification checks must be made, as appropriate. Verification checks may include, but are not limited to:
   - References on prior work performance
   - Confirmation of claimed academic and professional qualifications
   - Credit check
   - Professional license validation
   - Criminal background check
   - Salaries verification
   - Valid Virginia driver's license or identification

2. The type and number of verification checks conducted must be based on the employee's probable access to DMAS information systems containing PHI and their expected ability to modify or change such PHI.

3. The extent and type of screening will be based on DMAS' risk analysis process.

4. When defining a position, the DMAS Human Resources Division and the hiring manager must identify the security responsibilities and supervision required for the position. Security responsibilities include general responsibilities for implementing or maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of DMAS information systems or processes containing PHI.

5. When job candidates are provided by an agency, DMAS' contract with the agency must clearly state the agency's responsibilities for reviewing the candidates' backgrounds.

6. It is the responsibility of each DMAS Division that retains the services of a third party to ensure that the party or person(s) adheres to all appropriate DMAS policies.

7. All DMAS workforce members who access DMAS information systems containing PHI must sign a confidentiality agreement in which they agree not to provide PHI or to discuss confidential information to which they have access to unauthorized persons. New confidentiality agreements must be signed annually by DMAS workforce members who access DMAS information systems containing PHI.

8. All DMAS employees must sign a "conditions of employment" document that affirms their responsibility for the protection of the confidentiality, integrity, or availability of DMAS information systems and processes. The document must include the sanctions that may be applied if employees do not meet their responsibilities.

Reference: 45 CFR 164.308(a)(3)(ii)(B) (Addressable)
Related Policies: Authorization and/or Supervision
Workforce Security
Termination Procedures

Termination Procedures

HIPAA Security Rule Language: *Implement procedures for terminating access to electronic protected health information when the employment of a DMAS workforce member ends*

Purpose: This policy reflects DMAS' commitment to create and implement a formal, documented process for terminating access to electronic protected health information (PHI) when the employment of a DMAS workforce member ends

Policy:
1. DMAS has a formal, documented process for terminating access to electronic protected health information (PHI) when the employment of a workforce member ends.

2. When the employment of DMAS workforce members ends, their information systems privileges, both internal and remote, will be disabled or removed by the time of departure. DMAS information system privileges include, but are not limited to, workstation and server access, data access, network access, e-mail accounts, and inclusion on bulk e-mail lists. Consideration should also be given to physical access to areas where PHI is located.

3. When workforce members provide advance notice of their intention to leave DMAS, the Human Resources Division and the immediate manager or supervisor must give at least two days notice to the persons or Divisions responsible for DMAS information system privileges granted the departing workforce member. Receipt and response to such notices must be tracked and logged.

4. At a minimum, such tracking and logging will be securely maintained and provide the following information:
- Date and time notice of employee departure received
- Date of planned employee departure
- Brief description of access to be terminated
- Date, time, and description of actions taken

5. All DMAS workforce members must have their information system privileges automatically disabled after their user ID or access method has had 30 days of inactivity (example: when an external consultant ceases supplying services to DMAS without providing appropriate notification). All such privileges that are disabled in this manner must be reviewed to ensure that the inactivity is not due to termination of employment. If termination is the reason for inactivity, there must be review of situation to ensure that all access to PHI (or ability to physical access information) has been eliminated.

6 When workforce members depart from DMAS, they must return all DMAS supplied equipment by the time of departure. Such equipment includes, but is not limited to:

- Portable computers
- Personal digital assistants (PDAs)
- Name identification access badges
- Building, desk or office keys
- Parking access cards
- Security tokens
- Cell phones
- Travel credit cards

7. The return of all such equipment must be tracked, logged and must be securely maintained. At a minimum, such tracking and logging must provide the following information:
    - Date and time
    - Work force member's name
    - Brief description of returned items

8. If a departing workforce member has used cryptography on DMAS data, they must make the cryptographic keys available to appropriate management by the time of departure.

9. As appropriate, all physical security access codes used to protect DMAS information systems that are known by a departing workforce member must be deactivated or changed. For example, the PIN to a keypad lock that restricts entry to a DMAS facility containing information systems with PHI must be changed if a workforce member who knows the PIN departs.

10. A workforce member who departs from DMAS must not retain, give away, or remove from DMAS premises any DMAS information (this does not apply to copies of information provided to the public or copies of correspondence directly related to the terms and conditions of employment). All other DMAS information in the possession of the departing workforce member must be provided to the person's immediate supervisor at the time of departure.

11. When DMAS workforce members' employment ends, their computers' resident files must be promptly reviewed by their immediate supervisors to determine the appropriate transfer or disposal of any confidential information.

12. Special attention must be paid to situations where a departing employee poses a risk to information or systems at DMAS. If a workforce member is to be terminated immediately, their information system privileges must be removed or disabled just before they are notified of the termination.

13. Periodic review of DMAS information system access privileges will be performed to ensure that this policy is being adhered to and that existing procedures are effective.

Regulatory Reference: 45 CFR 164.308(a)(3)(ii)(C) (Addressable)

Related Policies: Workforce Security
Authorization and/or Supervision
Workforce Clearance Procedure

Information Access Management

HIPAA Security Rule Language: *Implement policies and procedures for authorizing access to electronic protected health information (PHI).*

Purpose: This policy reflects DMAS' commitment to have a formal documented process for authorizing appropriate access to DMAS information systems containing PHI.

Policy:

1. Access to DMAS information systems containing PHI is be managed in order to protect the confidentiality, integrity and availability of PHI.

2. As defined in DMAS' **Access Authorization policy,** DMAS has a formal documented process for authorizing appropriate access to DMAS information systems containing PHI.

3. As defined in DMAS' **Access Establishment and Modification policy**, DMAS must have a formal, documented process for establishing, documenting, reviewing, and modifying access to DMAS information systems containing PHI.

Reference: 45 CFR 164.308(a)(4)(i) (Required)

Related Policies:
Access Authorization
Access Establishment and Modification
Facility Access Controls
Access Control and Validation Procedures

Access Authorization

HIPAA Security Rule Language: *Implement policies and procedures for granting access to PHI, for example, through access to a workstation, transaction, program, process, or other mechanism*

Purpose: This policy reflects DMAS' commitment to have a formal documented process for authorizing appropriate access to DMAS information systems containing PHI.

Policy:
1. DMAS has a formal documented process for granting access to DMAS information systems that contain PHI. At a minimum, the process includes:
   - Procedure for granting different levels of access to DMAS information systems containing PHI.
   - Procedure for tracking and logging authorization of access to DMAS information systems containing PHI.
   - Procedure for regularly reviewing and revising, as necessary, authorization of access to DMAS information systems containing PHI.

2. DMAS workforce members must not be allowed access to information systems containing PHI until properly authorized.

3. The type and extent of access authorized to DMAS information systems containing PHI must be based on risk analysis

4. DMAS information system owners/custodians or their chosen delegates must define and authorize all access to DMAS information systems containing PHI that is entrusted to them. Such information system owners/custodians and delegates must be formally designated and documented.

5. Access to DMAS information systems containing PHI must be authorized only for DMAS workforce members having a need for specific information in order to accomplish a legitimate task. All such access is defined and documented. Such access is regularly reviewed and revised as necessary.

6. DMAS workforce members must not attempt to gain access to DMAS information systems containing PHI for which they have not been given proper authorization.

Reference: 45 CFR 164.308(a)(4)(ii)(B) (Addressable)

Related Policies: Information Access Management,
Access Establishment and Modification
Facility Access Controls
Access Control and Validation Procedures

Access Establishment and Modification

HIPAA Security Rule Language: *Implement policies and procedures that, based upon the covered entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.*

Purpose: This policy reflects DMAS' commitment to have a formal, documented process for establishing, documenting, reviewing, and modifying access to DMAS information systems containing PHI.

Policy:

1. DMAS must have a formal, documented process for establishing, documenting, reviewing, and modifying access to DMAS information systems containing PHI. The process must be based on DMAS' access authorization policy. At a minimum, the process must include:
   - Procedure for establishing different levels of access to DMAS information systems containing PHI.
   - Procedure for documenting levels of access established to DMAS information systems containing PHI.
   - Procedure for regularly reviewing DMAS workforce member access privileges to DMAS information systems containing PHI.
   - Procedure for modifying DMAS workforce member access privileges to DMAS information systems containing PHI.

2. Only properly authorized and trained DMAS workforce members may access DMAS information systems containing PHI. Such access must be established via a formal, documented process. At a minimum, this process must include:
   - Identification and definition of permitted access methods
   - Identification and definition of length of time that access will be granted
   - Procedure for both granting a workforce member an access method (e.g., password or token) and changing an existing access method
   - Procedure for managing access rights in a distributed and networked environment
   - Appropriate tracking and logging of activities by authorized workforce members on DMAS information systems containing PHI

3. Where appropriate, security controls or methods that allow access to be established to DMAS information systems containing PHI must include, at a minimum:
   - Unique user identifiers (user IDs) that enable individual users to be uniquely identified. User IDs must not give any indication of the user's privilege level. Common or shared identifiers must not be used to gain access to DMAS information systems containing PHI. When unique user identifiers are insufficient or inappropriate, shared identifiers may be used to gain access to DMAS information systems not containing PHI.
   - The prompt removal or disabling of access methods for persons and entities that no longer need access to DMAS PHI.
   - Verification that redundant user identifiers are not issued.

4. Access to DMAS information systems containing PHI must be limited to DMAS workforce members who have a need for specific PHI in order to perform their job responsibilities.

5. DMAS workforce members must not provide access to DMAS information systems containing PHI to unauthorized persons

6. Appropriate DMAS information system owners/custodians or their designated delegates must regularly review workforce member access rights to DMAS information systems containing PHI to ensure that they are provided only to those who have a need for specific PHI in order to accomplish a legitimate task. Such rights must be revised as necessary.

7. All revisions to DMAS workforce member access rights must be tracked and logged and must be securely maintained. At a minimum, such tracking and logging must provide the following information:

- Date and time of revision
- Identification of workforce member whose access is being revised
- Brief description of revised access right(s)
- Reason for revision
- Who authorized the revision
- Who implemented the revision

Reference: 45 CFR 164.308(a)(4)(ii)(C) (Addressable)

Related Policies: Information Access Management
Access Authorization
Facility Access Controls
Access Control and Validation Procedures

Security Awareness and Training

HIPAA Security Rule Language: *Implement a security awareness and training program for all members of a covered entity's workforce (including management)*

1. *Security reminders (A)*
2. *Protection from malicious software (A)*
3. *Log-on monitoring (A)*
4. *Password management (A)*

Purpose: This policy reflects DMAS' commitment to provide regular security awareness and training to its workforce members.

Policy:

1. Each workforce member who has access to DMAS information systems must understand how to protect the confidentiality, integrity, and availability of the systems.

2. DMAS must develop, implement, and regularly review a formal, documented program for regularly providing appropriate security training and awareness to workforce members.

3. All DMAS workforce members, both remote and onsite, must be provided with sufficient regular training and supporting reference materials to enable them to appropriately protect DMAS information systems. Such training may be provided at DMAS facility locations or via remote training methods. Such training must include, but is not limited to:

- All appropriate DMAS information security policies, procedures and standards.
- The secure use of DMAS information systems (e.g., logon procedures, allowed software).
- Significant risks to DMAS information systems and data.
- DMAS legal and business responsibilities for protecting its information systems and data.
- Security best practices (e.g., how to construct a good password, how to report a security incident).

4. All new DMAS employees will receive appropriate security training before being provided with access or accounts on DMAS information systems. After such training, each employee must verify that he or she has received the training, understood the material presented, and agree to comply with it.

5. Business associates must be informed of DMAS security policies and procedures on a regular basis. Such awareness can occur through contract language or other means.

6. Third-party persons who access DMAS information systems or data must be informed of DMAS security policies and procedures. It is the responsibility of each DMAS employee who retains the services of third-party individuals to ensure that these individuals adhere to all appropriate DMAS policies. Such responsibility may include verifying third-party individuals have attended security training or providing them with appropriate security training or reference materials.

7 All DMAS information security policies and procedures must be readily available for reference and review by appropriate employees, business associates, and third-party workers

8 All DMAS workforce members responsible for implementing safeguards to protect information systems must receive formal training that enables them to stay abreast of current security practices and technology.

9 As defined in DMAS' **Security Reminders policy**, DMAS must provide regular security information and awareness to its workforce members.

10 As defined in DMAS' **Protection from Malicious Software policy**, DMAS must regularly train and remind its workforce members about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems and data.

11 As defined in DMAS' **Log-on Monitoring policy**, DMAS must regularly train and remind its workforce members about its process for monitoring logon attempts and reporting discrepancies.

12 As defined in DMAS' **Password Management policy**, DMAS must regularly train and remind its workforce members about its process for creating, changing and safeguarding passwords.

Reference: 45 CFR 164.308(a)(5)(i) (Required)

Related Policies: Security Reminders
Protection from Malicious Software
Log-on Monitoring
Password Management

Security Reminders

HIPAA Security Rule Language: *Implement periodic security updates*

Purpose: This policy reflects DMAS' commitment to provide regular security information and awareness to its workforce members.

Policy:

1. DMAS must make certain that all of its workforce members, including those who work remotely, are regularly reminded of information security risks and how to follow DMAS security policies. Additionally, workforce members must be provided with information about DMAS security procedures and how to use DMAS information systems in ways that minimize possible security risks.

2. On a regular basis, DMAS must provide (at DMAS or via remote methods) all of its workforce members information and reminders on topics including, but not limited to:
   - DMAS information security policies.
   - Significant DMAS information security controls and processes.
   - Significant risks to DMAS information systems and data.
   - Security best practices (e.g., how to choose a good password, how to report a security incident).
   - DMAS' information security legal and business responsibilities (e.g. HIPAA, business associate contracts).

3. In addition to providing regular information security awareness, DMAS must provide (at DMAS or via remote methods) security information and awareness to all of its workforce members when any of the following events occur:
   - Significant revisions to DMAS' information security policies or procedures.
   - Significant new information security controls are implemented at DMAS.
   - Substantial changes are made to significant DMAS information security controls.
   - Significant changes occur to DMAS' information security legal or business responsibilities.
   - Significant new threats or risks arise against DMAS information systems or data.

4. DMAS Compliance and Security Officer is responsible for ensuring that workforce members receive regular security information and awareness.

5. Methods for providing security information and awareness can include, but are not limited to:
   - Email reminders
   - Posters
   - Letters
   - Workforce member meetings
   - Security days
   - Screen savers
   - Information system logon messages
   - Newsletter articles

- Paycheck messages

Reference: 45 CFR 164.308(a)(5)(ii)(A) (Addressable)

Related Policies: Security Awareness and Training
Protection from Malicious Software
Logon Monitoring
Password Management

Protection from Malicious Software

HIPAA Security Rule Language: *Implement procedures for guarding against, detecting, and reporting malicious software.*

Purpose: This policy reflects DMAS' commitment to provide regular training and awareness to its employees about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems.

Policy:

1. DMAS must be able to effectively detect and prevent malicious software, particularly viruses, worms and malicious code, and etc.

2. DMAS must develop, implement, and regularly review a formal, documented process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems and data. All DMAS workforce members must be regularly trained and reminded about this process.

3. At a minimum, DMAS' malicious software prevention, detection and reporting process must include:
   - Installation and regular updating of antivirus software on all DMAS information systems
   - Examination of data on electronic media and data received over networks to ensure that it does not contain malicious software.
   - The examination of all electronic mail attachments and data downloads for malicious software before use on DMAS information systems.
   - Procedures for members of the workforce to report suspected or known malicious software attacks.
   - An appropriate disaster recovery plan for recovering from malicious software attacks.
   - Procedures to verify that all information relating to malicious software is accurate and informative.
   - Procedures to ensure that DMAS workforce members do not modify web browser security settings without appropriate authorization.
   - Procedures to ensure that unauthorized software is not installed on DMAS information systems.

4. At a minimum, DMAS protection from malicious software training and awareness must cover topics including, but not limited to:
   - How to identify malicious software.
   - How to report malicious software.
   - How to effectively use antivirus software.
   - How to avoid downloading or receiving malicious software.
   - How to identify malicious software hoaxes.

5 Unless appropriately authorized, DMAS workforce members must not bypass or disable antivirus software.

Reference: 45 CFR 164 308(a)(5)(ii)(B) (Addressable)

Related Policies:
Security Awareness and Training
Security Reminders
Protection from Malicious Software
Log-on Monitoring
Password Management

Logon Monitoring

HIPAA Security Rule Language: *Implement procedures for monitoring logon attempts and reporting discrepancies*

Purpose: This policy reflects DMAS' commitment to regularly train and remind its workforce members about its process for monitoring logon attempts and reporting discrepancies.

Policy:

1. DMAS must develop, implement, and regularly review a formal, documented process for monitoring logon attempts and reporting discrepancies. All DMAS workforce members must be regularly trained and reminded about this process.

2. Access to all DMAS information systems must be via a secure logon process. At a minimum, the process must:
   - Not display information system or application identifying information until the logon process has been successfully completed.
   - Display a notice that the computer must only be accessed by authorized users.
   - Not provide help messages during the logon procedure that would assist an unauthorized user.
   - Validate logon information only when all data has been inputted. If an error arises, the system must not indicate which part of the data is correct or incorrect.
   - Limit the number of unsuccessful logon attempts allowed.

3. DMAS information systems' logon process must include the ability to:
   - Record unsuccessful logon attempts.
   - After a specific number of failed logon attempts, enforce a time delay before further logon attempts are allowed or reject any further attempts without authorization from an appropriate DMAS employee.
   - Limit the maximum time allowed for the logon procedure.
   - Display the following information on completion of a successful logon:
     - Date and time of the previous successful logon.

4. At a minimum, DMAS logon monitoring training and awareness must cover topics including, but not limited to:
   - How to effectively use DMAS secure logon processes.
   - How to detect logon discrepancies.
   - How to report logon discrepancies.

Reference: 45 CFR 164.308(a)(5)(ii)(C) (Addressable)

Related Policies: Security Reminders
Protection from Malicious Software
Password Management

Password Management

HIPAA Security Rule Language: *Implement procedures for creating, changing, and safeguarding passwords.*

Purpose: This policy reflects DMAS' commitment to provide regular training and awareness to its workforce members about creating, changing, and safeguarding passwords.

Policy:

1. DMAS must develop, implement, and regularly review a formal, documented process for appropriately creating, changing and safeguarding passwords used to validate a user's identity and establish access to its information systems and data. All DMAS workforce members must be regularly trained and reminded about this process.

2. At a minimum, DMAS' password management system must:
   - Require the use of individual passwords to maintain accountability.
   - Where appropriate, allow workforce members to select and change their own passwords.
   - Require unique passwords that meet the standards defined by the DMAS Office of Compliance and Security.
   - Require regular password changes.
   - Not display passwords in clear text when they are being input into an application.
   - Require the storage of passwords in encrypted form using a one-way encryption algorithm.
   - Require passwords to be given to users in a secure manner.
   - Require the changing of default vendor passwords following installation of software.

3. DMAS password creation standards must require at least the following:
   - Passwords must have a minimum length of eight characters.
   - Passwords must not be based on something that can be easily guessed or obtained using personal information (e.g., names, favorite sports team, etc.)
   - Passwords must be composed of a mix of numeric and alphabetical characters.

4. At a minimum, DMAS password management training and awareness must involve requirements for use of information systems including, but not limited to:
   - The importance of keeping passwords confidential and not sharing them with those who ask.
   - The need to avoid maintaining a paper record of passwords, unless the record can be stored securely.
   - Changing passwords whenever there is any indication of possible information system or password compromise.
   - DMAS' password standards.
   - The importance of not using the same password for personal and business accounts.
   - The importance of changing passwords at regular intervals and avoiding re-using old passwords.
   - Changing temporary passwords at the first logon.

- Not including passwords in any automated logon process (e.g., stored in a macro or function key).
- Ensuring that DMAS workforce members understand that all activities involving their user identification and password will be attributed to them.

Reference: 45 CFR 164.308(a)(5)(ii)(D) (Addressable)

Related Policies: Security Reminders

Protection from Malicious Software
Logon Monitoring
Password Management

Security Incident Procedures

HIPAA Security Rule Language: *Implement policies and procedures to address security incidents.*

Purpose: This policy reflects DMAS' commitment to implement policies and procedures for detecting and responding to security incidents.

Policy:

1. DMAS must have a formal, documented process for quickly and effectively detecting and responding to security incidents that may impact the confidentiality, integrity, or availability of DMAS information systems. At a minimum, the process must include the following:
   - A security incident response team (SIRT) and a formal procedure enabling DMAS workforce members to report a security incident to appropriate persons including potential reporting to the Information Security Officer.
   - Formal process for analyzing and identifying the cause(s) of a security incident.
   - Formal process for activation of the SIRT and procedure for communication with all DMAS workforce members affected by or responding to a security incident.
   - Formal procedure for collecting evidence of a security incident.
   - Formal mechanisms for evaluating security incidents and implementing appropriate mitigations to prevent further recurrence.
   - Regular training and awareness of DMAS workforce members about all security incident policies and procedures.
   - Regular risk analysis of DMAS information systems.

2. All DMAS actions to respond to and recover from security incidents must be carefully and formally controlled. At a minimum, formal procedures must ensure that:
   - All actions taken are intended to minimize the damage of a security incident and prevent further damage.
   - Only authorized and appropriately trained DMAS employees are allowed access to affected information systems in order to respond to or recover from a security incident.
   - All actions taken are carefully documented, reported to appropriate DMAS management and reviewed in a timely manner.

3. DMAS workforce members must report any observed or suspected security incidents as quickly as possible via DMAS security incident reporting procedure.

4. DMAS must have mechanisms for quantifying and monitoring the types, volumes and costs of security incidents. This information should be used to identify the need for improved or additional security controls.

5. DMAS' Compliance and Security Officer, in cooperation with the appropriate department manager, is authorized to investigate any and all alleged violations of DMAS security policies, and to take appropriate action to mitigate the infraction and apply sanctions as warranted.

Reference: 45 CFR 164.308(a)(6)(i) (Required)

Related Policies: Response and Reporting

Response and Reporting

HIPAA Security Rule Language: *Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes*

Purpose: This policy reflects DMAS' commitment to effectively detect and respond to security incidents in order to protect the confidentiality, integrity, and availability of its information systems.

Policy:

1. DMAS must be able to effectively detect and respond to security incidents in order to protect the confidentiality, integrity, and availability of its information systems.

2. DMAS must organize and maintain a security incident response team (SIRT) that will be DMAS' primary coordinator of security incident reporting and response. The SIRT must provide accelerated notification, damage control, and problem correction services when a security incident occurs. The specific responsibilities and scope of the SIRT must be defined in a charter.

3. DMAS' SIRT must create and document a formal security incident reporting procedure, which must be regularly reviewed and revised as necessary. The SIRT must provide DMAS workforce members with an easy to use and effective process for reporting security incidents. All DMAS workforce members must be regularly made aware of this process.

4. A DMAS workforce member must not prevent another member from reporting a security incident.

5. The SIRT must appropriately respond to all security incidents that are reported to it via the DMAS security incident reporting process.

6. When responding to an incident, the SIRT must take all appropriate actions to ensure that the confidentiality, integrity, and availability of DMAS information systems have not been compromised. Such actions can include, but are not limited to, temporarily removing an information system from the DMAS network, requesting access to an information system or viewing data.

7. All SIRT actions that will significantly affect DMAS workforce members must be defined by procedures that clearly detail decision-making processes and implementation steps.

8. Whenever evidence shows that a DMAS information system has been subject to a security incident, an investigation must be conducted by the DMAS SIRT. Such investigations should provide sufficient information to ensure that:
   - Vulnerabilities that lead to the incident(s) are identified.
   - Appropriate security controls are established to mitigate the above vulnerabilities.

9. DMAS' SIRT must create and document formal guidelines on security incident evidence collection. Such guidelines must be provided to all appropriate DMAS personnel. These guidelines must be regularly reviewed and revised as necessary.

10. For purposes of analysis and possible prosecution, DMAS must collect appropriate evidence regarding security incidents.

Reference: 45 CFR 164.308(a)(6)(ii) (Required)

Related Policies: Security Incident Procedures

Contingency Plan

HIPAA Security Rule Language: *Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain PHI*

Purpose: This policy reflects DMAS' commitment to effectively prepare for and respond to emergencies or disasters in order to protect the confidentiality, integrity and availability of its information systems.

Policy:

1. DMAS must have a formal process for both preparing for and effectively responding to emergencies and disasters that damage the confidentiality, integrity or availability of its information systems.

2. At a minimum, the process must include:
   - Regular analysis of the criticality of DMAS information systems.
   - Development and documentation of a disaster and emergency recovery strategy consistent with DMAS' business objectives and priorities.
   - Development and documentation of a disaster recovery plan that is in accordance with the above strategy.
   - Development and documentation of an emergency mode operations plan that is in accordance with the above strategy.
   - Regular testing and updating of the disaster recovery and emergency mode operations plans.

3. DMAS' disaster and emergency response process must reduce the disruption to DMAS information systems to an acceptable level through a combination of preventative and recovery controls and processes. Such controls and processes must identify and reduce risks to DMAS information systems, limit damage caused by disasters and emergencies and ensure the timely resumption of significant information systems and processes. Such controls and processes must be commensurate with the value of the information systems being protected or recovered.

4. DMAS workforce members must receive regular training and awareness on DMAS' disaster preparation and disaster and emergency response processes.

5. As described in DMAS' **Application and Data Criticality Analysis policy,** DMAS must have a formal process for defining and identifying the criticality of its information systems.

6. As described in DMAS' **Data Backup policy**, all PHI on DMAS information systems and electronic media must be regularly backed up and securely stored.

7. As described in DMAS' **Disaster Recovery Plan policy**, DMAS must create and document a disaster recovery plan to recover its information systems if they are impacted by a disaster.

8. As described in DMAS' **Emergency Mode Operations Plan policy**, DMAS must have a formal, documented emergency mode operations plan to enable the continuance of crucial business processes that protect the security of its information systems containing PHI during and immediately after a crisis situation.

9. As described in DMAS' **Testing and Revision Procedures policy**, DMAS must conduct regular testing of its disaster recovery plan to ensure that it is up to date and effective.

Regulatory Reference: 45 CFR 164.308(a)(7)(i) (Required)

Related Policies:
Data Backup Plan
Disaster Recovery Plan
Emergency Mode Operation Plan
Testing and Revision Procedure
Applications and Data Criticality Analysis

Data Backup Plan

HIPAA Security Rule Language: *Establish and implement procedures to create and maintain retrievable exact copies of PHI.*

Purpose: This policy reflects DMAS' commitment to backup and securely store all PHI on its information systems and electronic media.

Policy:
1. DMAS must have a formal, documented backup plan for its information systems. At a minimum, the plan must:
   - Identify information systems and electronic media to be backed up.
   - Provide a backup schedule.
   - Identify where backup media are stored and who may access them.
   - Outline restoration procedures.
   - Identify who is responsible for ensuring the backup of information systems and electronic media.

2. Backup copies of PHI stored at secure, remote location must be accessible to authorized DMAS employees for prompt retrieval of the information.

3. The backup media containing PHI at the remote backup storage site must be given an appropriate level of physical and environmental protection consistent with the standards applied to PHI physically at DMAS.

4. Restoration procedures for DMAS electronic media and information systems containing PHI must be regularly tested to ensure that they are effective and that they can be completed within the time allotted in DMAS disaster recovery plan.

5. The retention period for backup of PHI on DMAS information systems and electronic media and any requirements for archive copies to be permanently retained must be defined and documented.

6. Risk analysis should be used to determine and document the maximum amount of loss that may occur if backup of DMAS information systems and electronic media is disrupted. Such analysis should be used to determine if all appropriate and reasonable measures are being used to backup DMAS information systems and electronic media.

Reference: 45 CFR 164.308(a)(7)(ii)(A) (Required)

Related Policies:
Contingency Plan
Disaster Recovery Plan
Emergency Mode Operation Plan
Testing and Revision Procedure
Applications and Data Criticality Analysis

Disaster Recovery Plan

HIPAA Security Rule Language: *Establish (and implement as needed) procedures to restore any loss of data*

Purpose: This policy reflects DMAS' commitment to implement a disaster recovery plan to recover its information systems if they are impacted by a disaster.

Policy:

1. DMAS must create and document a disaster recovery plan to recover its information systems if they are impacted by a disaster. The plan must be reviewed regularly and revised as necessary.

2. At a minimum, the recovery plan must include:
   - The conditions for activating the plan.
   - Identification and definition of DMAS workforce member responsibilities.
   - Resumption procedures (manual and automated) which describe the actions to be taken to return DMAS information systems to normal operations within required time frames.
   - The order in which information systems will be recovered.
   - Notification and reporting procedures.
   - Procedure(s) for allowing appropriate employees physical access to DMAS facilities so that they can implement recovery procedures in the event of a disaster.
   - A maintenance schedule that specifies how and when the plan will be tested, as well as the process for maintaining the plan.

3. DMAS workforce members must receive regular training on the disaster recovery plan.

4. All appropriate DMAS workforce members must have a current copy of the plan and an appropriate number of current copies of the plan must be kept off-site.

Reference: 45 CFR 164.308(a)(7)(ii)(B) (Required)

Related Policies: Contingency Plan
Data Backup Plan
Emergency Mode Operation Plan
Testing and Revision Procedure
Applications and Data Criticality Analysis

Emergency Mode Operation Plan

HIPAA Security Rule Language: *Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of PHI while operating in emergency mode.*

Purpose: This policy reflects DMAS' commitment to have an emergency mode operations plan for protecting its information systems containing PHI during and immediately after a crisis situation.

Policy:

1. DMAS must have a formal, documented emergency mode operations plan for protecting its information systems containing PHI during and immediately after a crisis situation. At a minimum, the plan must:
   - Identify significant processes and controls that protect the confidentiality, integrity, and availability of PHI on DMAS information systems.
   - Identify and prioritize emergencies that may impact DMAS information systems containing PHI.
   - Define procedures for how DMAS will respond to specific emergencies that impact information systems containing PHI.
   - Define procedures for how DMAS, during and immediately after a crisis situation, will maintain the processes and controls that ensure the availability, integrity and confidentiality of PHI on DMAS information systems.
   - Define a procedure that ensures that authorized employees can enter DMAS facilities to enable continuation of processes and controls that protect PHI while DMAS is operating in emergency mode.

2. DMAS workforce members must receive regular training and awareness on the emergency mode operations plan.

3. All appropriate DMAS workforce members must have a current copy of the plan and an appropriate number of current copies of the plan must be kept off-site.

Reference: 45 CFR 164.308(a)(7)(ii)(C) (Required)

Related Policies:
Contingency Plan
Data Backup Plan
Disaster Recovery Plan
Emergency Mode Operation Plan
Testing and Revision Procedure
Applications and Data Criticality Analysis

Testing and Revision Procedure

HIPAA Security Rule Language: *Implement procedures for periodic testing and revision of contingency plans.*

Purpose: This policy reflects DMAS' commitment to regularly test its information technology contingency plan.

Policy:

1. DMAS must conduct regular testing of its contingency plan to ensure that it is current and operative. DMAS must have a formal process defining how and when its plan will be tested.

2. As appropriate, the following types of tests can be performed on DMAS' contingency plan:
   - Paper test: A detailed walk-through of the plan that typically includes tasks such as validating the vendor call and notification lists and reviewing end user procedures.
   - Limited scope test: A test of one or more components of the disaster recovery plan. Typical test tasks include using backup tapes to restore selected information systems at a remote recovery facility or on test machines within DMAS; and testing communications between DMAS and its alternate/recovery facility or facilities.
   - Simulated full-scale disaster: A complete test of the disaster recovery plan. The test will likely interrupt normal DMAS operations and should only be attempted after significant limited scope testing and after determination that such a test would not impact operations. Such testing typically requires executive management support and extensive planning.

3. The results of such tests must be formally documented and presented to appropriate DMAS management. The contingency plan must be revised as necessary to address issues or gaps identified in the testing process.

4. DMAS' contingency plan must be kept current via a formal change control process. Examples of events that must result in an update of the plan include, but are not limited to:
   - Change in disaster recovery personnel.
   - Change in contact information for disaster recovery personnel.
   - Significant change(s) to DMAS' technical or physical infrastructure.
   - Change in key suppliers or customers.
   - Significant change in threats to DMAS facilities or information systems.

Regulatory Reference: 45 CFR 164.308(a)(7)(ii)(D) (Addressable)

Related Policies:
Contingency Plan
Data Backup Plan
Disaster Recovery Plan
Emergency Mode Operation Plan
Applications and Data Criticality Analysis

Applications and Data Criticality Analysis

HIPAA Security Rule Language: *Assess the relative criticality of specific applications and data in support of other contingency plan components*

Purpose: This policy reflects DMAS' commitment to conduct a regular analysis of the criticality of its information systems.

Policy:

1. DMAS must have a formal, documented process for defining and identifying the criticality of its information systems and the data contained within them. At a minimum, the process must include:
   - An inventory of all DMAS information systems and identification of dependencies between DMAS information systems.
   - A methodology for determining the criticality of DMAS' information systems
   - Identification and likelihood of risks that threaten DMAS information systems and data.
   - Documentation of the impact to these risks have to DMAS services, processes and business objectives if specific DMAS information systems are unavailable for different periods of time (e.g., 1 hour, 1 day).
   - Identification of maximum time periods that DMAS information systems can be unavailable and prioritization of DMAS information systems according to their criticality to DMAS ability to function at normal levels.

2. The prioritization of DMAS information systems must be based on an analysis of the impact to DMAS services, processes and business objectives if disasters or emergencies cause specific information systems to be unavailable for particular periods of time.

3. The criticality analysis must be conducted with significant involvement from the systems owners, administrators, and users of DMAS information systems and processes.

4. The criticality analysis can be conducted by either DMAS employee(s) or by a qualified third-party firm who should understand the interdependencies among DMAS' information systems and processes.

5. Results from the analysis must be documented, presented to appropriate DMAS management and must be securely maintained. Any change in status of information systems and/or the data contained within them must be reflected in DMAS disaster recovery plan.

Reference: 45 CFR 164.308(a)(7)(ii)(E) (Addressable)

Related Policies: Data Backup Plan
Disaster Recovery Plan
Emergency Mode Operation Plan
Testing and Revision Procedure

Evaluation

HIPAA Security Rule Language: *Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the security of PHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.*

Purpose: This policy reflects DMAS' commitment to regularly conduct a technical and non-technical evaluation of its security controls and processes to document compliance with its security policies and the HIPAA Security Rule.

Policy:

1. DMAS must regularly conduct a technical and non-technical evaluation of its security controls and processes to document its compliance with its security policies and the HIPAA Security Rule.

2. The evaluation may be carried out by an appropriate DMAS business unit such as the Compliance and Security Officer, the Auditor of Public Accounts, or a third-party organization that has appropriate skills and experience.

3. The evaluation must be formal and defined and at a minimum include:
   - A detailed review of DMAS' security policies, procedures and standards to determine whether they are effective and appropriate.
   - A gap analysis of the requirements of DMAS' security policies, procedures and standards and actual practices.
   - Identification of the risks to DMAS information systems.
   - Assessment of the appropriateness of DMAS security controls compared to the risks to DMAS information systems.
   - Testing of all significant DMAS security controls to ensure that hardware and software controls have been correctly implemented. Such testing must be carried out only by authorized and appropriately trained persons.

4. The results of the evaluation must be formally documented and presented to appropriate DMAS management. The document must be securely maintained.

5. All appropriate areas and employees within DMAS must be included in the evaluation. These should include the following:
   - System owners and administrators
   - System users/custodians
   - Management

6. After the initial evaluation, DMAS must conduct a thorough technical and non-technical evaluation of its security controls and processes when environmental or operational changes occur which significantly impact the confidentiality, integrity, or availability of its PHI. Such changes include but are not limited to:
   - Significant security incidents to DMAS information systems.
   - Significant new threats or risks to DMAS information systems.
   - Significant changes to the organizational or technical infrastructure of DMAS.

- Significant changes to DMAS information security requirements or responsibilities.

7. Such evaluations must be formally defined and at a minimum include:
   - A detailed review of DMAS' security policies, procedures and standards to determine whether they are still effective and appropriate.
   - Identification of the risks to DMAS information systems after the environmental or operational changes.
   - Assessment of the appropriateness of DMAS security controls compared to the risks to DMAS information systems.
   - Testing of all DMAS security controls affected by the changes to ensure that hardware and software controls remain correctly and appropriately implemented. Such testing must be carried out only by authorized and appropriately trained persons.

8. The results of all such evaluations must be formally documented and presented to appropriate DMAS management. The document must be securely maintained.

Reference: 45 CFR 164.308(a)(8)(i) (Required)

Related Policies: DMAS Information Security Policy

Business Associate Contracts and Other Arrangements

HIPAA Security Rule Language: *A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that that the business associate will appropriately safeguard the information*

Purpose: This policy reflects DMAS' commitment to only permit a business associate to create, receive, maintain, or transmit PHI on its behalf if there is a written agreement between the two parties which provides assurances that the business associate will appropriately safeguard the information.

Policy:

1. DMAS will permit a business associate to create, receive, maintain, or transmit PHI on its behalf only if there is a written agreement between the two parties which ensures that the business associate will appropriately and reasonably safeguard the information.

2. When another entity is acting as a business associate of DMAS, the business associate must appropriately and reasonably protect the PHI that it creates, receives, maintains or transmits on DMAS behalf.

3. Exception: When required by law, DMAS may permit a business associate to receive, create, maintain, or transmit PHI on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of the business associate contract. DMAS must make a good faith attempt to obtain satisfactory assurances that the business associate will safeguard the DMAS' PHI, as required by the business associate contract, and to document the attempt and the reasons that these assurances cannot be obtained.

4. The transmission of PHI by DMAS to a health care provider concerning the treatment of an individual does not require a business associate agreement.

5. All business associate agreements must be documented and must follow the standard business associate agreement language of DMAS.

6. New contracts with existing business associates do not have to be obtained specifically for this purpose, if existing written contracts adequately address the applicable requirements or can be amended to do so.

Reference: 45 CFR 164.308(b)(1); 45 CFR 164.308(b)(2) (Required)

NOTE: This policy combines both the Standard and its Implementation Specification

Related Policies: DMAS Privacy Policies

This page left intentionally blank

Policies on the Standards for Physical Safeguards

This page left intentionally blank

Facility Access Controls

HIPAA Security Rule Language: *Implement policies and procedures to limit physical access to a covered entity's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.*

Purpose: This policy reflects DMAS' commitment to prevent unauthorized physical access to its facilities while ensuring that properly authorized access is allowed.

Policy:

1. DMAS must protect the confidentiality, integrity, and availability of its information systems by preventing unauthorized physical access, tampering, and theft to the systems and to the facilities in which they are located, while ensuring that properly authorized access is allowed.

2. DMAS' information systems containing PHI must be physically located in areas where unauthorized access is minimized.

3. DMAS must perform an inventory of all physical access controls used to protect information systems at its facilities. The inventory report must be stored in a secure manner (e.g., appropriate file access permissions or a locked drawer).

4. The perimeter of a building or site containing DMAS information systems with PHI must be physically sound; the external walls of the site should be solidly constructed and all external doors must have appropriate protections against unauthorized access.

5. Physical barriers must, if necessary, be extended from actual floor to actual ceiling to prevent unauthorized entry. Doors and windows should be locked when unattended. External protection should be considered for windows, particularly at ground level.

6. DMAS' delivery and loading areas must be controlled to prevent unauthorized access. Where possible, the following controls must be used:
   - Access to a holding area from outside of the building must be restricted to identified and authorized persons.
   - The holding area must be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building.
   - The external door(s) of a holding area must be secured when the internal door is opened.

7. The level of protection provided for DMAS' information systems containing PHI must be commensurate with that of identified risks. An assessment of the risks to DMAS facilities and information systems containing PHI must be conducted periodically. The risk assessment report must be stored in a secure manner.

8. The risk assessment report must place DMAS' information systems containing PHI into defined categories of risk such as:

   - Highly Sensitive – areas where large amounts of PHI are stored and maintained. Access to such areas requires security controls such as card keys, visitor escort, and sign-in sheets.

- Sensitive – areas that have a high concentration of visitors and terminals which access PHI. Security controls used in these areas include locked closets and securely located workstations.

9. All physical access rights to DMAS areas where information systems containing PHI are maintained must be clearly defined and documented. Such rights must be provided only to DMAS workforce members having a need for specific access in order to accomplish the responsibilities of their positions.

10. All physical access rights to DMAS areas where information systems containing PHI are maintained must be regularly reviewed and revised as necessary.

11. All DMAS workforce members must visibly wear the organization's employee identification. Employees should report unescorted strangers or anyone not wearing visible identification.

12. All visitors must show proper identification and sign in prior to gaining physical access to DMAS areas where information systems containing PHI are located.

13. As defined in DMAS' **Contingency Operations policy**, DMAS must have formal, documented procedures for allowing authorized workforce members to enter its facilities to take necessary actions as defined in its disaster recovery and emergency mode operations plans.

14. As defined in DMAS' **Facility Security Plan policy**, DMAS must have a facility security plan that details how it will protect its facilities and equipment.

15. As defined in DMAS' **Access Control and Validation Procedures policy**, DMAS must implement procedures to control and validate individuals' access to DMAS facilities based on their roles or functions.

16. As defined in DMAS' **Maintenance Records policy**, DMAS must document all repairs and modifications to the physical components of its facilities that are related to security.

Reference: 45 CFR 164.310(a)(1) (Required)

Related Policies: Contingency Operations
Facility Security Plan
Access Control and Validation Procedures
Maintenance Records

Contingency Operations

HIPAA Security Rule Language: *Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency*

Purpose: This policy reflects DMAS' commitment to ensure that, in the event of a disaster or emergency, appropriate individuals can enter its facilities to take necessary actions defined in its Disaster Recovery and Emergency Mode Operations Plans.

Policy:

1. DMAS must ensure that, in the event of a disaster or emergency, appropriate persons can enter its facility to take necessary actions defined in its Disaster Recovery and Emergency Mode Operations Plans.

2. Based on its Emergency Mode Operations Plan, DMAS must develop, implement, and regularly review a formal, documented procedure that ensures that authorized employees can enter the facility to enable continuation of processes and controls that protect PHI while DMAS is operating in emergency mode. Such employees or roles must be defined in DMAS Emergency Mode Operations Plan. Actions taken by such employees must be appropriately tracked and logged as defined in DMAS Emergency Mode Operations Plan.

3. All access rights to DMAS processes and controls which protect PHI must be clearly defined and documented. Such rights must be provided only to DMAS employees having a need for specific access in order to accomplish a legitimate task related to contingency operations. All such access rights must be regularly reviewed and revised as necessary.

4. In the event of an emergency, only authorized DMAS employees may administer or modify processes and controls which protect PHI contained on information systems. Such employees or roles must be defined in DMAS Emergency Mode Operations Plan.

Reference: 45 CFR 164.310(a)(2)(i) (Addressable)

Related Policies: Facility Security Plan
Access Control and Validation Procedures
Maintenance Records

Facility Security Plan

HIPAA Security Rule Language: *Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.*

Purpose: This policy reflects DMAS' commitment to maintain a facility security plan for protecting its facilities and all information systems contained within them.

Policy:

1. DMAS must protect the confidentiality, integrity, and availability of its information systems by preventing unauthorized physical access, tampering and theft.

2. DMAS must maintain and regularly review a formal, documented facility security plan that describes how its facilities and equipment within them will be appropriately protected. The plan must be revised as necessary.

3. DMAS 'facility security plan must include appropriate safeguards for all equipment containing electronic protected health information (PHI).

4. The facility security plan must be based on a risk assessment that assesses the risks to DMAS facilities and the information systems contained within.

5. At a minimum, DMAS' facility security plan must address the following:
   - Identification of DMAS information systems to be protected from unauthorized physical access, tampering, and theft.
   - Identification of processes and controls used to protect DMAS information systems from unauthorized physical access, tampering, and theft.
   - Actions to be taken if unauthorized physical access, tampering, or theft attempts are made against DMAS information systems.
   - Identification and definition of DMAS workforce member responsibilities.
   - Notification and reporting procedures
   - A maintenance schedule that specifies how and when the plan will be tested, as well as the process for maintaining the plan.

6. All appropriate DMAS workforce members must have a current copy of the plan. An appropriate number of current copies of the plan must be maintained off-site.

Reference: 45 CFR 164.310(a)(2)(ii) (Addressable)

Related Policies: Contingency Operations
Access Control and Validation Procedures
Maintenance Records
Facility Access Controls

Access Control and Validation Procedures

HIPAA Security Rule Language: *Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.*

Purpose: This policy reflects DMAS' commitment to control and validate physical access to its facilities containing information systems having PHI or software programs that can access PHI.

Policy:

1. DMAS will determine and document all areas considered sensitive due to the nature of the PHI that is stored or available within them.

2. After documenting sensitive areas, access rights to such areas should be given only to workforce members who have a need for specific physical access in order to accomplish a legitimate task.

3. Roles or functions of DMAS workforce members and others (e.g., the public) who may be granted physical access rights to sensitive areas must be defined and documented.

4. All access rights to DMAS facilities containing information systems having PHI or software programs that can access PHI must be regularly reviewed and revised as necessary.

5. All physical access to sensitive facilities must be tracked, logged, stored in a secure manner and be regularly reviewed. At a minimum, such tracking and logging must provide:
   - Date and time of access
   - Name or user ID of person gaining access
   - Name of workforce member who granted access

6. DMAS workforce members must not attempt to gain physical access to DMAS sensitive facilities containing information systems having PHI or software programs that can access PHI for which they have not been given proper authorization.

7. DMAS workforce members must immediately report to appropriate management the loss or theft of any device (e.g., card or token) that enables them to gain physical access to such sensitive facilities.

8. DMAS workforce members must wear an identification badge when at DMAS facilities containing information systems having PHI or software programs that can access PHI and should be encouraged to report unknown persons not wearing such identification.

9. All visitors to sensitive facilities must show proper identification, state reason for need to access, and sign in prior to gaining access.

Reference: 45 CFR 164.310(a)(2)(iii) (Addressable)

Related Policies: Facility Access Controls

Contingency Operations
Facility Security Plan
Maintenance Records

Maintenance Records

HIPAA Security Rule Language: *Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).*

Purpose: This policy reflects DMAS' commitment to document all repairs and modifications to the physical components of its facilities that are related to the protection of PHI.

Policy:

1. DMAS must document all repairs and modifications to the physical components of its facilities that are related to security of PHI. Physical components include, but are not limited to, automated physical access systems, locks, doors and walls.

2. DMAS must conduct an inventory of all the physical components of its facilities that are related to the protection of PHI. Inventory results must be documented and stored in a secure manner (e.g., on a computer with appropriate file access permissions or in a locked drawer).

3. Repairs or modifications to any DMAS physical component listed in the above inventory must be documented. At a minimum, the documentation must include:
   - Date and time of repair or modification
   - Reason for repair or modification
   - Person(s) performing the repair or modification
   - Outcome of repair or modification

4 Such documentation must be securely maintained.

Reference: 45 CFR 164.310(a)(2)(iv) (Addressable)

Related Policies: Facility Access Controls
Contingency Operations
Facility Security Plan
Access Control and Validation Procedures

Workstation Use

HIPAA Security Rule Language: *Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access PHI*

Purpose: This policy reflects DMAS' commitment to appropriately use and protect its workstations.

Policy:

1. DMAS workstations must be used only for authorized purposes: to support the research, education, clinical, administrative, and other functions of DMAS. Such use demonstrates respect for intellectual property, ownership of data, security controls, and individuals' rights to privacy.

2. All workforce members who use DMAS workstations must take all reasonable precautions to protect the confidentiality, integrity, and availability of PHI contained on the workstations.

3. Workforce members must not use DMAS workstations to engage in any activity that is either illegal under local, state, federal, or international law or is in violation of DMAS policy.

4. Activities that workforce members must not perform while using DMAS workstations include, but are not limited to:

- Violations of the rights to privacy of protected healthcare information of DMAS' PHI.
- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property or similar laws or regulations. This includes, but is not limited to, the installation or distribution of "pirated" or other inappropriately licensed software products.
- Unauthorized copying of copyrighted material, including but not limited to digitization and distribution of photographs from magazines, books, or other copyrighted sources and copyrighted music.
- Purposeful introduction of malicious software onto a workstation or network (e.g., viruses, worms, Trojan horses, etc.).
- Actively engaging in procuring or transmitting material that is in violation of DMAS sexual harassment or hostile workplace policies.
- Making fraudulent offers of products, items, or services.
- Purposefully causing security breaches. Security breaches include, but are not limited to, accessing electronic data that the workforce member is not authorized to access or logging into an account that he or she is not authorized to access. DMAS employees that perform this activity as part of their defined job are exempt from this prohibition.
- Performing any form of network monitoring that will intercept electronic data not intended for the workforce member. DMAS employees that perform this activity as part of their defined job are exempt from this prohibition.
- Circumvent or attempt to avoid the user authentication or security of any DMAS workstation or account. Employees that perform this activity as part of their defined job are exempt from this prohibition.

5. Access to all DMAS workstations containing PHI must be controlled with a username and password or an access device such as a token.

6. Access to all DMAS workstations with PHI must be authenticated via a process that includes, at a minimum:

- Unique user IDs that enable users to be identified and tracked. Group IDs may only be used to access DMAS workstations not containing PHI.
- The prompt removal of workstation access privileges for workforce members who whose employment or contracted service with DMAS has ended.
- Verification that redundant user IDs are not issued.

7. All password-based access control systems on DMAS workstations must mask, suppress, or otherwise obscure the passwords so that unauthorized persons are not able to observe them.

8. DMAS workforce members must not share passwords with others. If a DMAS workforce member believes that someone else is inappropriately using a user-ID or password, they must immediately notify their manager.

9. Where possible, the initial password(s) issued to a new DMAS workforce member must be valid only for the new user's first logon to a workstation. At initial logon, the user must be required to choose another password. Where possible, this same process must be used when a workforce member's password is reset.

10. DMAS workstations containing PHI must be physically located in such a manner as to minimize the risk that unauthorized individuals can gain access to them.

11. The display screens of all DMAS workstations containing PHI must be positioned such that information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception, public, or other related areas.

12. VITA approved antivirus software must be installed on workstations to prevent transmission of malicious software. Such software must be regularly updated.

13. DMAS workforce members must activate their workstation locking software whenever they leave their workstation unattended for 10 minutes or more. DMAS workforce members must shut down their equipment when their shifts are complete.

14. Connections from one workstation to another computer must be logged off after the session is completed.

15. Workstations removed from DMAS premises must be protected with security controls equivalent to those for on-site workstations.

16. Special precautions must be taken with portable workstations such as laptops. The following guidelines must be followed with such systems:

- PHI must not be stored on a portable workstation unless such information is appropriately protected. DMAS approved encryption must be used.
- Locking software for unattended laptops must activate after 10 minutes.
- DMAS portable workstations must be carried as carry-on (hand) baggage when workforce members use public transport. They must be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile).

Reference: 45 CFR 164.310(b) (Required)

Related Policies: Workstation Security

Workstation Security

HIPAA Security Rule Language: *Implement physical safeguards for all workstations that access PHI, to restrict access to authorized users.*

Purpose: This policy reflects DMAS' commitment to prevent unauthorized physical access to workstations that can access PHI while ensuring that authorized workforce members have appropriate access.

Policy:

1. DMAS must prevent unauthorized physical access to workstations that can access PHI and ensure that authorized workforce members have appropriate access.

2. DMAS workstations containing PHI must be located in locations that minimize the risk of unauthorized access to them.

3. DMAS workforce members must take reasonable measures to prevent viewing PHI on workstations by unauthorized persons. Such measures include but are not limited to:
   - Locating workstations and peripheral devices (printer, modem, scanner, etc.) in secured areas not accessible to unauthorized persons
   - Positioning monitors or shielding workstations so that data shown on the screen is not visible to unauthorized persons.

5. The level of physical protection provided for DMAS workstations containing PHI must be commensurate with that of identified risks. An assessment of the risks to DMAS workstations that can access PHI must be conducted and the risk assessment report must be securely maintained.

6. Unauthorized DMAS workforce members must not attempt to gain physical access to workstations that can access PHI.

7. DMAS workforce members must report loss or theft of any access device (such as a card or token) that allows them physical access to DMAS areas having workstations that can access PHI.

8. All DMAS portable workstations must be securely maintained when in the possession of workforce members. Such workstations must be handled as carry-on (hand) baggage on public transport. They must be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile).

Reference: 45 CFR 164.310(c) (Required)

Related Policies: Workstation Use

Device and Media Controls

HIPAA Security Rule Language: *Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility*

Purpose: This policy reflects DMAS' commitment to appropriately control information systems and electronic media containing PHI moving into, out of and within its facilities.

Policy:

1. PHI located on DMAS information systems or electronic media must be protected against damage, theft, and unauthorized access. This includes both PHI received by DMAS and created within DMAS. PHI must be consistently protected and managed through its entire life cycle, from origination to destruction.

2. Information systems and electronic media for which this policy applies include, but are not limited to, computers (both desktop and laptop), floppy disks, backup tapes, CD-ROMs, zip drives, portable hard drives, PDAs, flash memory, etc.

3. All DMAS electronic media that contains PHI must be clearly marked as confidential and should have a unique tracking number assigned by the creator attached to it.

4. DMAS must regularly conduct a formal, documented process that ensures consistent control of all electronic media and information systems containing PHI that is created, sent, received or destroyed by DMAS.

5. DMAS must conduct an organization-wide inventory to identify all of its information systems and electronic media that contain PHI. Inventory results must be documented and stored in a secure manner, e.g., on a computer with appropriate file access permissions or in a locked drawer.

6. Access to information systems and electronic media containing PHI at DMAS must be provided only to authorized DMAS workforce members who have a need for specific access in order to accomplish a legitimate task.

7. DMAS workforce members must not attempt to access, duplicate or transmit electronic media containing PHI for which they have not been given appropriate authorization.

8. All DMAS information systems and electronic media containing PHI must be located and stored in secure environments that are protected by appropriate security barriers and entry controls. The level of these controls should be commensurate with identified risks to the electronic media and information systems.

9. As defined in DMAS' **Disposal policy**, all information systems and electronic media containing PHI must be disposed of securely and safely when no longer required.

10. As defined in DMAS' **Media Re-use policy**, all PHI on DMAS information systems and electronic media must be carefully removed before the media or information systems are made available for re-use.

11. As defined in DMAS' **Accountability** policy, all information systems and electronic media containing PHI that are received or removed from DMAS or move within its facilities must be appropriately tracked and logged.

12. As defined in DMAS' **Data Backup and Storage** policy, backup copies of all PHI located on DMAS information systems or electronic media must be regularly made and stored securely.

Reference: 45 CFR 164.310(d)(1) (Required)

Related Policies: Disposal, Media Re-use
Accountability
Data Backup and Storage

Disposal

HIPAA Security Rule Language: *Implement policies and procedures to address the final disposition of PHI, and/or the hardware or electronic media on which it is stored.*

Purpose: This policy reflects DMAS' commitment to appropriately dispose of information systems and electronic media containing PHI when it is no longer needed.

Policy:

1. All DMAS information systems and electronic media containing PHI must be disposed of properly when no longer needed for legitimate use. This disposal must include the PHI received by DMAS and created within DMAS. Careless disposal of such information systems and media could result in PHI being revealed to unauthorized persons.

2. Information systems and electronic media to which this policy applies include, but are not limited to: computers (both desktop and laptops), floppy disks, backup tapes, CD-ROMs, zip drives, portable hard drives, flash memory, etc.

3. Disposal of all DMAS electronic media and information systems containing PHI must be tracked and logged. At a minimum, such tracking and logging must provide the following information:
   - Date and time of disposal
   - Who performed the disposal
   - Brief description of media or information systems that was disposed

4. If an information system or electronic medium containing PHI is to be reused within DMAS (or for other entities), its previous data must be completely removed with erase tool(s) that have been approved by the DMAS Information Management Division in compliance with the VITA requirements.

5. An information system or electronic medium containing PHI that is disposed of permanently must be physically destroyed after its previous data has been completely removed with erase tool(s) that have been approved by the DMAS Information Management Division in compliance with the VITA requirements.

5. Destruction of DMAS electronic media includes, at minimum, shredding or burning. An industrial data destruction service or facility may be used. Care must be taken to select a suitable contractor with adequate controls and experience, including the handling of confidential information.

Reference: 45 CFR 164.310(d)(2)(i) (Required)

Related Policies: Device and Media Controls
Media Re-use
Accountability
Data Backup and Storage

Media Re-use

HIPAA Security Rule Language: *Implement procedures for removal of PHI from electronic media before the media are made available for re-use.*

Purpose: This policy reflects DMAS' commitment to erase all PHI from electronic media before its re-use.

Policy:

1. All PHI on DMAS electronic media must be removed before such media can be re-used. Failure to remove PHI could result in it being revealed to unauthorized persons. This includes both PHI received by DMAS and created within DMAS.

2. DMAS must maintain and regularly review a formal, documented process that ensures all PHI on electronic media is removed before the media are re-used.

3. Electronic media to which this policy applies include, but are not limited to, floppy disks, backup tapes, CD-ROMs, zip drives, portable hard drives, flash memory, etc.

4. PHI on DMAS electronic media must be removed with erase tools that have been approved by the DMAS Information Management Division in compliance with the VITA requirements.

Reference: 45 CFR 164.310(d)(2)(ii) (Required)

Related Policies: Device and Media Controls
Disposal
Accountability,
Data Backup and Storage

Accountability

HIPAA Security Rule Language: *Maintain a record of the movements of hardware and electronic media and any person responsible therefore.*

Purpose: This policy reflects DMAS' commitment to appropriately track and log the movements of PHI on information systems and electronic media and to hold DMAS workforce members accountable for such movement.

Policy:

1. All movement of DMAS information systems and electronic media containing PHI into and out of its facilities will be tracked and logged. Those responsible for such movement must take all appropriate and reasonable actions to protect PHI. This includes both PHI received by DMAS and created within DMAS.

2. Information systems and media for which this policy applies include, but are not limited to, computers (both desktop and laptops), floppy disks, backup tapes, CD-ROMs, zip drives, portable hard drives, PDAs, flash memory, etc.

3. Workforce members should use only DMAS approved and tracked electronic media to store PHI.

4. Unless appropriately protected and authorized, PHI must not be stored on DMAS workforce member home computers.

5. Appropriate DMAS management must authorize the use or sending of any information system or electronic media containing PHI outside DMAS' premises. Such authorization must be tracked and logged. At a minimum, such tracking and logging must provide the following information:
   - Date and time of movement of system or media
   - Brief description of person using or sending PHI on system or media
   - Brief description of where PHI is to be sent or how used
   - Name of person authorizing such transaction

Information should be regularly reviewed and stored in a secure manner, e.g., on a computer with appropriate file access permissions or in a locked drawer.

6. All receipts of electronic media and information systems containing PHI from outside DMAS premises (e.g. from the public or business partners) must be tracked and logged. At a minimum, such tracking and logging must provide the following information:
   - Date and time PHI received
   - Brief description of electronic media or information system containing PHI
   - Name of person(s) receiving PHI
   - Brief description of action taken with received PHI

7. DMAS employees and affiliates who move electronic media or information systems containing PHI are responsible for the subsequent use of such items and must take all appropriate and reasonable actions to protect them against damage, theft, and unauthorized access

Reference: 45 CFR 164.310(d)(2)(iii) (Addressable)

Related Policies: Device and Media Controls
Media Re-use
Disposal
Data Backup and Storage

Data Backup and Storage

HIPAA Security Rule Language: *Create a retrievable, exact copy of PHI, when needed, before movement of equipment.*

Purpose: This policy reflects DMAS' commitment to backup and securely store all PHI on its information systems and electronic media.

Policy:

1. Backup copies of all PHI on DMAS electronic media and information systems must be made regularly. This includes both PHI received by DMAS and created within DMAS.

2. Information systems and electronic media for which this policy applies include, but are not limited to, computers (both desktop and laptops), floppy disks, backup tapes, CD-ROMs, zip drives, portable hard drives, PDAs, flash memory, etc.

3. DMAS must have adequate backup systems that ensure that all such PHI can be recovered following a disaster or media failure. These systems must be regularly tested.

4. Backup of PHI on DMAS information systems and electronic media, together with accurate and complete records of the backup copies and documented restoration procedures, must be stored in a secure remote location, at a sufficient distance from DMAS facilities to escape damage from a disaster at DMAS.

5. Backup and restoration procedures for DMAS electronic media and information systems containing PHI must be regularly tested to ensure that they are effective and that they can be completed within a reasonable amount of time.

Reference: 45 CFR 164.310(d)(2)(iv) (Addressable)

Related Policies:
Device and Media Controls
Media Re-use
Disposal
Accountability

This page left intentionally blank

Policies on the Standards for Technical Safeguards

This page left intentionally blank

Access Control

HIPAA Security Rule Language: *Implement policies and procedures for electronic information systems that maintain PHI to allow access only to those persons or software programs that have been granted access rights as specified in the Information Access Management Standard.*

Purpose: This policy reflects DMAS' commitment to purchase and implement information systems that comply with DMAS' information access management policies.

Policy:

1. DMAS must purchase and implement information systems that comply with DMAS' information access management policy.

2. All current DMAS information systems that do not currently comply with DMAS' information access management policy must be identified and evaluated according to DMAS' risk analysis process.

3. As appropriate, DMAS information systems must support one or more of the following types of access control to protect the confidentiality, integrity and availability of PHI contained on DMAS information systems:
   - User based
   - Role or function based
   - Context based

4. DMAS information systems must support a formal process for granting appropriate access to DMAS information systems containing PHI. At a minimum, the process must include:
   - Procedure for granting different levels of access to DMAS information systems containing PHI.
   - Procedure for tracking and logging authorization of access to DMAS information systems containing PHI.
   - Procedure for regularly reviewing and revising, as necessary, authorization of access to DMAS information systems containing PHI.

5. DMAS workforce members and software programs cannot be granted access to information systems containing PHI until properly authorized.

6. As appropriate, security controls or methods that allow access to DMAS information systems containing PHI must include, at a minimum:
   - Unique user identifiers (user IDs) that enable persons and identities to be uniquely identified. User IDs must not give any indication of the user's privilege level. Group identifiers must not be used to gain access to DMAS information systems containing PHI. When unique user identifiers are insufficient or inappropriate, group identifiers may be used to gain access to DMAS information systems not containing PHI.
   - A secret identifier (password).
   - The prompt removal or disabling of access methods for persons and entities that no longer need access to DMAS PHI.
   - Verification that redundant user identifiers are not issued.

7. Access to DMAS information systems containing PHI must be limited to DMAS workforce members and software programs that have a need to access specific information in order to accomplish a legitimate task.

8. DMAS workforce members must not provide access to DMAS' information systems containing PHI to unauthorized persons.

9. Appropriate DMAS information system owners/custodians or their designated delegates must regularly review workforce member and software program access rights to DMAS information systems containing PHI to ensure that access is granted only to those having a need for specific information in order to accomplish a legitimate task. Such rights must be revised as necessary.

10. All revisions to DMAS workforce members and software program access rights must be tracked and logged and must be securely maintained. At a minimum, such tracking and logging must provide the following information:

- Data and time of revision
- Identification of workforce member or software program whose access is being revised
- Brief description of revised access right(s)
- Reason for revision
- Who authorized the revision
- Who made the revision

11. As defined in DMAS' **Unique User Identification policy**, access to DMAS information systems must be via user identifiers that uniquely identify workforce members and enable activities with each identifier to be traced to a specific person or entity.

12. As defined in DMAS' **Emergency Access Procedure policy**,DMAS must have a formal, documented emergency access procedure enabling authorized workforce members to obtain required PHI during an emergency.

13. As defined in DMAS' **Automatic Logoff policy**, DMAS workforce members must end electronic sessions between information systems that contain or can access PHI when such sessions are finished, unless they can be secured by an appropriate locking method.

14. As defined in DMAS' **Encryption and Decryption policy**, where risk analysis shows it is necessary, appropriate encryption must be used to protect the confidentiality, integrity and availability of PHI contained on DMAS information systems.

Reference: 45 CFR 164.312(a)(1) (Required)

Related Policies:
Unique User Identification
Emergency Access Procedure
Automatic Logoff
Encryption and Decryption
Information Access Management
Access Authorization
Access Establishment and Modification
Facility Access Controls
Access Control and Validation Procedures

Unique User Identification

HIPAA Security Rule Language: *Assign a unique name and/or number for identifying and tracking user identity*

Purpose: This policy reflects DMAS' commitment to assign a unique name or number to identify and track the identity of workforce members who access DMAS information systems.

Policy:

1. DMAS information systems must grant users access via unique identifiers that:
   - identify workforce members or users, and
   - allow activities performed on information systems to be traced back to a particular individual through tracking of unique identifiers.

2. Unique identifiers must not give any indication of the user's privilege level.

3. Unique identifiers can include but are not limited to:
   - Biometric identification
   - Workforce member names
   - Exclusive numbers (e.g., PIN)

4. Group user identifiers must not be used to gain access to DMAS information systems that contain PHI. When unique user identifiers are insufficient or inappropriate, group identifiers may be used only to gain access to DMAS information systems that do not contain PHI.

5. Standard user naming practices (e.g., first initial, last name) must not be used for DMAS workforce members who require access to highly sensitive DMAS information systems (e.g., firewalls, core routers). Such practices can enable an attacker to target certain user names. Instead, a DMAS information security office approved user naming practice must be used to create user names for such users.

6. Verification that redundant user identifiers are not issued (i.e., only one user ID per person, per application). Exceptions must be documented.

Reference: 45 CFR 164.312(a)(2)(i) (Required)

Related Policies: Access Control
Emergency Access Procedure
Automatic Logoff
Encryption and Decryption

Emergency Access Procedure

HIPAA Security Rule Language: *Establish (and implement as needed) procedures for obtaining necessary PHI during an emergency.*

Purpose: This policy reflects DMAS' commitment to have an emergency access procedure enabling authorized workforce members to obtain required PHI during an emergency.

Policy:

1. DMAS must have a formal, documented emergency access procedure enabling authorized workforce members to obtain required PHI during an emergency. At a minimum, the procedure must:
   - Identify and define which DMAS workforce members are authorized to access PHI during an emergency (e.g., systems owners/custodians, users).
   - Identify and define manual and automated methods to be used by authorized DMAS workforce members to access PHI during an emergency.
   - Identify and define appropriate logging and auditing that must occur when authorized DMAS workforce members access PHI during an emergency.

2. DMAS must have a formal, documented emergency access procedure enabling DMAS workforce members to access the minimum PHI necessary to treat patients in the event of an emergency. Such access must be authorized by appropriate DMAS management.

3. DMAS workforce members must receive regular training and awareness on the emergency access procedure.

4. All appropriate DMAS workforce members must have a current copy of the procedure and an appropriate number of current copies of the procedure must be kept off-site.

Reference: 45 CFR 164.312(a)(2)(ii) (Required)

Related Policies:
Access Control
Automatic Logoff
Encryption and Decryption
Unique User Identification
Emergency Mode Operations Plan

Automatic Logoff

HIPAA Security Rule Language: *Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity*

Purpose: This policy reflects DMAS' commitment to develop and implement procedures for terminating electronic sessions on information systems that contain or access PHI.

Policy:

1. DMAS workforce members must end electronic sessions on information systems that contain or can access PHI when such sessions are completed, unless the information system is secured by an appropriate locking method, e.g. a password protected screen saver.

2. Electronic sessions on information systems that contain or can access PHI and which lack appropriate locking methods must be automatically terminated after 10 minutes of inactivity.

3. Exceptions to DMAS information system required inactivity timeout must be approved by DMAS information security office after risk analysis has been conducted.

4. DMAS workforce members must activate their workstation locking software whenever they leave their workstation unattended for 10 minutes or more.

5. DMAS workforce members must log off from or lock their workstation(s) when their shift is complete.

Reference: 45 CFR 164.312(a)(2)(iii) (Addressable)

Related Policies:
Access Control
Emergency Access Procedure
Encryption and Decryption
Unique User Identification

Encryption and Decryption

HIPAA Security Rule Language: *Implement a mechanism to encrypt and decrypt PHI.*

Purpose: This policy reflects DMAS' commitment to appropriately use encryption to protect the confidentiality, integrity and availability of PHI at rest contained on DMAS information systems.

Policy:

1. When risk analysis indicates it is necessary, appropriate encryption must be used to protect the confidentiality, integrity, and availability of PHI at rest contained on DMAS information systems.

2. At a minimum, DMAS' risk analysis must consider the following factors when determining whether or not specific PHI must be encrypted:
   - The sensitivity of the PHI
   - The risks to the PHI
   - The expected impact to DMAS functionality and workflow if the PHI is encrypted
   - Alternative methods available to protect the confidentiality, integrity and availability of the PHI.

3. All encryption used to protect the confidentiality, integrity and availability of PHI contained on DMAS information systems must be approved by DMAS' Security Advisory Committee.

4. Encryption must be used to protect the confidentiality, integrity, and availability of PHI stored on DMAS portable workstations (i.e., laptops, etc.) and removable media.

5. Encryption must be used to protect the confidentiality, integrity, and availability as specified in DMAS' **Transmission Security policy**.

6. DMAS must protect all of its cryptographic keys against modification and destruction; its secret and private keys must be protected against unauthorized disclosure.

7. DMAS must have a formal, documented process for managing the process to encrypt PHI on DMAS information systems.

8. No Division will implement encryption of data without the knowledge and approval of the Compliance and Security Officer and the Backup Information Security Officer.

10. DMAS will maintain documentation with regards to when encryption is utilized.

Reference: 45 CFR 164.312(a)(2)(iv) (Addressable)

Related Policies:
Access Control
Emergency Access Procedure
Automatic Logoff
Unique User Identification

Audit Controls

HIPAA Security Rule Language: *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI.*

Purpose: This policy reflects DMAS' commitment to use appropriate audit controls on its information systems that contain or use PHI.

Policy:

1. DMAS must be able to record and examine significant activity on its information systems that contain or use PHI.

2. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on DMAS information systems that contain or use PHI. At a minimum, such mechanisms must provide the following information:
   - Date and time of significant activity
   - Origin of significant activity
   - Identification of user performing significant activity
   - Description of attempted or completed significant activity

3. The level and type of auditing mechanisms that must be implemented on DMAS information systems that contain or use PHI must be determined by DMAS' risk analysis process. Events that should be audited may include but are not limited to:
   - Access of certain data (e.g., sensitive PHI like HIV or mental health records)
   - Use of certain software programs or utilities
   - Use of a privileged account
   - Information system start-up or stop
   - Failed authentication attempts

4. Logs created by audit mechanisms implemented on DMAS information systems must be reviewed regularly. The frequency of such review must be determined by DMAS' risk analysis process.

5. DMAS must develop and implement a formal process for audit log review. At a minimum, the review process must include:
   - Definition of which workforce members will review logs
   - Procedure for defining how significant log events will be identified and reported
   - Definition of audit record retention criteria

6. DMAS workforce members should not review audit logs that pertain to their own system activity.

Reference: 45 CFR 164.312(b) (Required)

Related Policies: Security Incident Procedures
Response and Reporting

Integrity

HIPAA Security Rule Language: *Implement policies and procedures to protect PHI from improper alteration or destruction.*

Purpose: This policy reflects DMAS' commitment to appropriately protect the integrity of all PHI contained on its information systems.

Policy:

1. DMAS must appropriately protect the integrity of all PHI contained on its information systems. Such PHI must be protected from improper alteration or destruction.

2. DMAS must implement a formal, documented process for appropriately protecting the integrity of all PHI contained on its information systems. At a minimum, the process must include: ensuring that the methods and controls used to protect integrity are effective and do not significantly impact DMAS functionality and workflow and define:
   - how DMAS will detect and report instances of attempted or successful improper alteration or destruction of DMAS PHI.
   - how DMAS will respond to instances of attempted or successful improper alteration or destruction of DMAS PHI.
   - when and how unnecessary DMAS PHI can be destroyed. Such destruction must be conducted only by properly authorized DMAS workforce members in accordance with DMAS records retention schedule.

3. Only properly authorized and trained DMAS workforce members may access and use PHI on DMAS information systems. Such access and use must be provided only to DMAS workforce members having a need for access to specific PHI in order to accomplish a legitimate task.

4. Such access and use must be clearly defined and documented and be regularly reviewed by systems owners/custodians and revised as necessary.

5. Methods used to protect the integrity of PHI contained on DMAS information systems must ensure that the value and state of the PHI is maintained and it is protected from unauthorized modification and destruction. Such controls include but are not limited to:
   - Checksums
   - Digital signatures
   - Hash values
   - Encryption

Reference: 45 CFR 164.312(c)(1) (Required)

Related Policies: Mechanism to Authenticate PHI

Mechanism to Authenticate PHI

HIPAA Security Rule Language: *Implement electronic mechanisms to corroborate that PHI has not been altered or destroyed in an unauthorized manner.*

Purpose: This policy reflects DMAS' commitment to implement appropriate electronic mechanisms to confirm that PHI contained on DMAS information systems has not been altered or destroyed in an unauthorized manner.

Policy:

1. DMAS must implement appropriate electronic mechanisms to confirm that PHI contained on DMAS information systems has not been altered or destroyed in an unauthorized manner.

2. All electronic mechanisms used to protect the integrity of PHI contained on DMAS information systems must be approved by DMAS' Security Advisory Committee.

3. DMAS workforce members must receive regular training and awareness about the electronic mechanisms used to protect the integrity of PHI contained on DMAS information systems

Reference: 45 CFR 164.312(c)(2) (Addressable)

Related Policies: Integrity

Person or Entity Authentication

HIPAA Security Rule Language: *Implement procedures to verify that a person or entity seeking access to PHI is the one claimed.*

Purpose: This policy reflects DMAS' commitment to ensure that all persons or entities seeking access to DMAS PHI are appropriately authenticated before access is granted.

Policy:

1. DMAS must create and implement a formal, documented process for verifying the identity of a person or entity before granting them access to PHI. The process must be regularly reviewed and revised as necessary.

2. At a minimum, DMAS' authentication process must include the following:
   - Formal documented procedure(s) for both granting a person or entity an authentication method (e.g., password, biometrics, or token) or changing an existing authentication method.
   - All authentication identifiers used for access to DMAS PHI must be uniquely identifiable so activities using the identifier can be traced to an individual person or entity.
   - Formal documented procedures for detecting and responding to unusual or suspicious authentication activity.

3. DMAS must use an appropriate and reasonable system(s) to ensure that only properly authenticated persons and entities access its PHI. Such systems may include but are not limited to:
   - Biometric identification systems
   - Password systems
   - Personal identification number (PIN) systems
   - Telephone callback systems
   - Security token systems

4. When applicable, such authentication system(s) must include, at a minimum:
   - Unique user identifiers (user IDs) that enable persons and entities to be uniquely identified. User IDs must not give any indication of the user's privilege level. Group identifiers must only be used when unique user identifiers are insufficient or inappropriate. Group identifiers must be reviewed and approved by appropriate management. Group identifiers must not be used to gain access to DMAS information systems containing PHI.
   - A secret identifier (password).
   - The prompt removal or disabling of authentication methods for persons and entities that no longer need access to DMAS PHI.
   - Verification that redundant user identifiers are not issued.

5. All authentication methods must meet industry best practice standards. DMAS must provide employees with regular training and awareness about the authentication standard(s).

6. All authentication data, such as passwords and PINs, must be protected with appropriate access controls to prevent unauthorized access.

7. All password and PIN based authentication systems on DMAS information systems must mask, suppress, or otherwise obscure the passwords and PINs so that unauthorized persons are not able to observe them.

8. Methods (e.g., password or PIN) for authentication to DMAS information systems must not be built into logon scripts. All exceptions must be reviewed and approved by appropriate management.

9. DMAS employees must not share or reveal their authentication methods to others. Sharing an authentication method means the authorized user assumes responsibility for actions that another party takes with the disclosed method. A DMAS employee who believes that their authentication method is being inappropriately used must immediately notify his or her manager.

10. DMAS employees must immediately report the loss or theft of an access method (e.g., key card or security token) to appropriate management.

11. To prevent authentication by unauthorized persons, DMAS employees must activate their workstation locking software whenever they leave their workstation unattended for 10 minutes or more. Locking or timeout software must activate on all other DMAS information systems after 10 minutes or more of inactivity.

12. Authentication attempts to all DMAS information systems must be limited to no more than 5 attempts in 10 minutes. Authentication attempts that exceed the limit must result in:

- The relevant account being disabled for an appropriate period of time;
- The event being logged; and
- Notification of appropriate DMAS personnel.

Reference: 45 CFR 164.312(d) (Required)

Related Policies: Password Use and Management
Logon Monitoring
Security Awareness and Training

Transmission Security

HIPAA Security Rule Language: *Implement technical security measures to guard against unauthorized access to PHI that is being transmitted over an electronic communications network.*

Purpose: This policy reflects DMAS' commitment to appropriately protect the confidentiality, integrity, and availability of PHI and any other sensitive data that it transmits over electronic communications networks.

Policy:

1. DMAS must appropriately protect the confidentiality, integrity and availability of all PHI and sensitive data it transmits over electronic communications networks.

2 Unless risk analysis indicates that there is not significant risk when sending DMAS data over an electronic communications network, the data must be sent in encrypted form and have controls to safeguard the integrity of the data.

3. Encryption and integrity controls must always be used when highly sensitive DMAS data such as passwords or PHI are transmitted over electronic communications networks.

4. DMAS must implement a formal, documented process for how DMAS data requiring encryption and integrity controls will be transmitted over electronic communications networks. At a minimum, the process must include:

- A procedure for ensuring that the encryption and integrity controls are effective and do not significantly impact functionality and workflow between DMAS and data recipients.
- A procedure enabling data recipients to report instances of attempted or successful unauthorized access to DMAS data that is transmitted over an electronic communications network.
- A procedure defining how DMAS will respond to instances of attempted or successful unauthorized access to DMAS data that is transmitted over an electronic communications network.

5. As described in DMAS' **Encryption policy**, when risk analysis indicates it is necessary, appropriate encryption must be used to protect the confidentiality, integrity, and availability of DMAS PHI data transmitted over electronic communications networks.

6. As described in DMAS' **Integrity Controls policy**, when risk analysis indicates it is necessary, appropriate integrity controls must be used to protect the confidentiality, integrity, and availability of DMAS PHI data transmitted over electronic communications networks.

Reference: 45 CFR 164.312(e)(1) (Required)

Related Policies: Integrity Controls
Encryption

Integrity Controls

HIPAA Security Rule Language: *Implement security measures to ensure that electronically transmitted PHI is not improperly modified without detection until disposed of.*

Purpose: This policy reflects DMAS' commitment to use appropriate integrity controls to protect the confidentiality, integrity, and availability of DMAS data transmitted over electronic communications networks.

Policy:

1. When risk analysis indicates it is necessary, appropriate integrity controls must be used to protect the confidentiality, integrity and availability of DMAS PHI data transmitted over electronic communications networks.

2. Integrity controls must always be used when highly sensitive DMAS PHI data such as passwords are transmitted over electronic communications networks.

3. DMAS' integrity controls must ensure that the value and state of all transmitted data is maintained and the data is protected from unauthorized modification

Reference: 45 CFR 164.312(e)(2)(i) (Addressable)

Related Policies: Transmission Security
Encryption

Encryption

HIPAA Security Rule Language: *Implement a mechanism to encrypt PHI whenever deemed appropriate.*

Purpose: This policy reflects DMAS' commitment to appropriately use encryption to protect the confidentiality, integrity and availability of DMAS data transmitted over electronic communications networks.

Policy:

1. When risk analysis indicates it is necessary, appropriate encryption must be used to protect the confidentiality, integrity and availability of DMAS PHI data transmitted over electronic communications networks. The risk analysis must also be used to determine the type and quality of the encryption algorithm and the length of cryptographic keys.

2. Encryption must always be used when highly sensitive DMAS data such as passwords are transmitted over electronic communications networks.

3. All encryption used to protect the confidentiality, integrity and availability of DMAS PHI data transmitted over an electronic communications network must be approved by DMAS Security Advisory Committee.

Reference: 45 CFR 164.312(e)(2)(ii) (Addressable)

Related Policies: Transmission Security
Integrity Controls

This page left intentionally blank

Policies for the Other Standards

This page left intentionally blank

Policies and Procedures

HIPAA Security Rule Language: *Implement reasonable and appropriate policies and procedures to comply with the standards, the implementation specifications, or other requirements*

Purpose: This policy reflects DMAS' commitment to appropriately maintain, distribute and review the security policies and procedures it implements to comply with the HIPAA Security Rule.

Policy:

1. DMAS must establish and maintain organizational policies and procedures to address all requirements of the final HIPAA Security Rule.

2. DMAS must establish and maintain organizational policies and procedures to ensure and support the confidentiality, integrity, and availability of the Agency's PHI.

3. DMAS' workforce members must be informed of all policies and procedures that apply to them in their individual roles.

4. DMAS must establish policies and procedures for organizational security that incorporate the specific characteristics of DMAS with respect to:
   - the size, complexity, and capabilities of the Agency,
   - the Agency technical infrastructure, hardware, and software capabilities,
   - the cost of implementing security measures, and
   - the probability and criticality of potential risks to the Agency's PHI.

5. DMAS must ensure that its policies and procedures for security are compatible with the Agency's culture and strategic planning objectives.

6. DMAS must conduct an annual formal review of the policies and procedures for security and update them as necessary.

Reference: 45 CFR 164.316(a) (Required)

Related Policies: Documentation
Evaluation

Documentation

HIPAA Security Rule Language: *Maintain the policies and procedure implemented to comply with this in written form and review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.*

Purpose: This policy reflects DMAS' commitment to maintain written documentation of the Agency's actions and activities related to the implementation of security policies and procedures to comply with the HIPAA Security Rule.

Policy:

1. DMAS must maintain the security policies and procedures it implements to comply with the HIPAA Security Rule in written (paper or electronic) form.

2. If an action, activity or assessment is required by the HIPAA Security Rule to be documented, DMAS must maintain a written (paper or electronic) record of the action, activity, or assessment. Such records may include, but not be limited to:
   - Security Advisory Committee Minutes
   - Committee/task force Charters
   - Executive Memorandums
   - Quality Improvement Evaluations
   - Corrective Action Plans

3. DMAS must retain such required documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

4. DMAS must make such required documentation available to all workforce members responsible for implementing the policies and procedures to which the documentation pertains.

5. DMAS must periodically review the required documentation and update it as needed, in response to environmental or operational changes affecting the confidentiality, integrity or availability of its PHI.

Reference: 45 CFR 164.316(b); (Required)
164.316(b)(i); (Required)
164.316(b)(ii); (Required)
164.316(b)(iii) (Required)

Related Policies: Policies and Procedures
Evaluation

Appendix 1 - Security Standards Matrix - *Appendix A to Subpart C of Part 164*

Administrative Safeguards

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis § 164.308(a)(1)(ii)(A)	(R)
		Risk Management § 164.308(a)(1)(ii)(B)	(R)
		Sanction Policy § 164.308(a)(1)(ii)(C)	(R)
		Information System Activity Review § 164.308(a)(1)(ii)(D)	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision § 164.308(a)(3)(ii)(A)	(A)
		Workforce Clearance Procedure § 164.308(a)(3)(ii)(B)	(A)
		Termination Procedures § 164.308(a)(3)(ii)(C)	(A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function § 164.308(a)(4)(ii)(A)	(R)
		Access Authorization § 164.308(a)(4)(ii)(B)	(A)
		Access Establishment and Modification § 164.308(a)(4)(ii)(C)	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders § 164.308(a)(5)(ii)(A)	(A)
		Protection from Malicious Software § 164.308(a)(5)(ii)(B)	(A)
		Log-in Monitoring § 164.308(a)(5)(ii)(C)	(A)
		Password Management § 164.308(a)(5)(ii)(D)	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting § 164.308(a)(6)(ii)	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan § 164.308(a)(7)(ii)(A)	(R)
		Disaster Recovery Plan § 164.308(a)(7)(ii)(B)	(R)
		Emergency Mode Operation Plan § 164.308(a)(7)(ii)(C)	(R)
		Testing and Revision Procedure § 164.308(a)(7)(ii)(D)	(A)
		Applications and Data Criticality Analysis § 164.308(a)(7)(ii)(E)	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement § 164.308(b)(4)	(R)

Physical Safeguards

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations § 164.310(a)(2)(i)	(A)
		Facility Security Plan § 164.310(a)(2)(ii)	(A)
		Access Control and Validation Procedures § 164.310(a)(2)(iii)	(A)
		Maintenance Records § 164.310(a)(2)(iv)	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal § 164.310(d)(2)(i)	(R)
		Media Re-use § 164.310(d)(2)(ii)	(R)
		Accountability § 164.310(d)(2)(iii)	(A)
		Data Backup and Storage § 164.310(d)(2)(iv)	(A)

Technical Safeguards

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification § 164.312(a)(2)(i)	(R)
		Emergency Access Procedure § 164.312(a)(2)(ii)	(R)
		Automatic Logoff § 164.312(a)(2)(iii)	(A)
		Encryption and Decryption § 164.312(a)(2)(iv)	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate PHI § 164.312(c)(2)	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls § 164.312(e)(2)(i)	(A)
		Encryption § 164.312(e)(2)(ii)	(A)

This page left intentionally blank

Appendix 2

Procedure Template

Procedure Concept	Definition
Title	Establish what the topic of the procedure will be
Intent	Discuss what the procedure is attempting to accomplish
Scope	Briefly describe the process the procedure is going to cover (e.g., implementing a user –id request or responding to a user 800 call)
Responsibilities	Identify who is to perform what steps in procedure by job function not names
Sequence of events	To help user understand the timing and conditions for performing tasks identified in the procedure. (e.g., task executed at a specific time or when a specific condition is met)
Approvals	Identify any necessary approvals/signatures and when these approvals must be met; approvals to be obtained prior to the execution of the process
Prerequisites	List any preconditions that must be met before starting the procedures process
Definitions	Include discussion/of any terms and acronyms that are included in the body of the procedure
Equipment, tools, documentation required	Identify all equipment, tools, documents and anything else the individual executing the procedure will need to perform the tasks
Warnings	Some tasks, if operated or executed in improper sequence could cause harm to the enterprise. Identify those key tasks and review the importance of understanding exactly when the task is to be executed and under what set of circumstances
Precautions	Identify all steps to be taken to avoid problems or dangers (e.g., unplug before performing maintenance, or turn on before recording)
Procedure body	These are the actual steps to be performed in the execution of the process

This page left intentionally blank.